MATHEMATICS OF COMPUTATION
VOLUME 48, NUMBER 178
APRIL 1987, PAGES 751-755

On a Problem of A. Rotkiewicz

By Péter Kiss and Bui Minh Phong

Abstract. For any fixed positive integers a, $k \geqslant 2$ there are infinitely many composite integers n such that $a^{n-k} \equiv 1 \pmod{n}$.

1. Introduction. A. Rotkiewicz asked in his book the following question. "Let a, $k > 1$ be fixed positive integers. Do there exist infinitely many composite integers n such that $n \mid (a^{n-k} - 1)$?" [5, problem 18, p. 138]. It is well known that the answer is affirmative in the case $k = 1$; the numbers satisfying the condition are called pseudoprime numbers to base a. A general result was obtained by A. Makowski [2]: For any natural number $k \geqslant 2$ there are infinitely many composite n such that

$$a^{n-k} \equiv 1 \pmod{n} \tag{1}$$

for any positive integer a with $(a, n) = 1$. This result was proved earlier by D. C. Morrow [3] in the case $k = 3$. In his proof, Makowski showed that there are infinitely many integers n of the form $n = k \cdot p$ (where p is a prime) such that congruence (1) holds for any positive integer a if $(a, n) = 1$. Naturally, $(k, a) = 1$ for these numbers, and so the question remained unanswered if a and k are fixed and $(k, a) > 1$. In the cases $(k, a) > 1$, A. Rotkiewicz obtained two results: He proved that (1) has infinitely many solutions n if $k = 3$ and a is an arbitrarily fixed positive integer, or if $k = 2$ and $a = 2$ (see [5, Theorem 32, p. 129] and [6], respectively).

The aim of this paper is to give a general solution of the problem. We prove:

THEOREM. *Let a $(\geqslant 2)$ and k be fixed positive integers. Then there are infinitely many composite integers n such that*

$$a^{n-k} \equiv 1 \pmod{n}.$$

2. Auxiliary Results. We shall use some lemmas in the proof of our theorem.

LEMMA 1. *Let*

$$\Phi_n(x) = \prod_{d \mid n} (x^d - 1)^{\mu(n/d)}$$

be the nth cyclotomic polynomial, where μ is the Moebius function. If a and n are natural numbers with $a \geqslant 2$ and $n > 30$, then

$$\Phi_n(a) > n(2n + 1). \tag{2}$$

Received October 25, 1985.
1980 *Mathematics Subject Classification*. Primary 10A10.
Key words and phrases. Congruence, primitive prime divisor.

Proof. First we prove the inequality

$$\Phi_n(a) > a^{\frac{2}{3}\varphi(n)} \tag{3}$$

for every integer a, $n > 1$, where φ denotes the Euler function.

Let $\nu(n)$ denote the number of distinct prime factors of n. For integers $1 < n \leqslant 12$ and $n = 30$, using the definition of $\Phi_n(a)$, inequality (3) can be seen directly. For the others, separating the cases $\nu(n) = 1, 2, 3$, and $\nu(n) \geqslant 4$, it can be easily seen that

$$\tfrac{1}{3}\varphi(n) \geqslant 2^{\nu(n)-1}.$$

But G. D. Birkhoff and H. S. Vandiver [1] showed that

$$\Phi_n(a) > a^{\varphi(n)-2^{\nu(n)-1}}, \tag{4}$$

and so (3) indeed holds.

It is known that $\varphi(n) > n^{2/3}$ for $n > 30$ (see, e.g., [4, p. 38]); therefore, by (3) we have

$$\Phi_n(a) > a^{\frac{2}{3}n^{2/3}}$$

if $n > 30$. One can check that

$$a^{\frac{2}{3}n^{2/3}} > n(2n+1)$$

for $n \geqslant 99$ if $a = 2$, and for $n \geqslant 35$ if $a \geqslant 3$. In the case $a \geqslant 3$, inequality (2) can be seen directly for $n = 31$, 32, 33 and 34; thus we have to prove the lemma only for $a = 2$ and for integers n for which $30 < n < 99$.

If $n > 30$ and n is a prime or a prime power (i.e., $\nu(n) = 1$), then obviously

$$\Phi_n(2) > 2^{n/2} > n(2n+1).$$

If $\nu(n) = 2$, then $\varphi(n) \geqslant n(1 - \frac{1}{2})(1 - \frac{1}{3}) = n/3$, and by (4) we have

$$\Phi_n(2) > 2^{n/3-2} > n(2n+1)$$

for $n \geqslant 42$; by numerical calculation we can show that $\Phi_n(2) > n(2n+1)$ for $30 < n < 42$, too.

If $\nu(n) = 3$ then, similarly as above, $\varphi(n) \geqslant \frac{4}{15}n$ and

$$\Phi_n(2) > 2^{\frac{4}{15}n-4} > n(2n+1)$$

follow for $n \geqslant 64$. But there are only two integers $n = 42 = 2 \cdot 3 \cdot 7$ and $n = 60 = 2^2 \cdot 3 \cdot 5$ for which $\nu(n) = 3$ and $30 < n < 64$, and by numerical computation we get $\Phi_{42}(2) > 42 \cdot (2 \cdot 42 + 1)$ and $\Phi_{60}(2) > 60 \cdot (2 \cdot 60 + 1)$; thus the lemma holds in this case.

If $\nu(n) > 3$, then $n > 99$, which completes the proof of the lemma.

LEMMA 2. *Let a ($\geqslant 2$) be a natural number and let p ($\geqslant 3$) be a prime. If the number a belongs to the exponent $(p-1)/2$ modulo p (i.e., $p \mid (a^{(p-1)/2} - 1)$ but $p \nmid (a^i - 1)$ for $0 < i < (p-1)/2$), and $P(n)$ denotes the greatest prime factor of n with $P(1) = 1$, then*

$$\Phi_{(p-1)/2}(a) > p \cdot P\left(\frac{p-1}{2}\right), \tag{5}$$

unless $(p; a) = (3; 4), (5; 4), (5; 9), (7; 2), (7; 4), (13; 4), (17; 2)$ or $(41; 2)$.

Proof. Since $P((p-1)/2) \leqslant (p-1)/2$ by Lemma 1, inequality (5) holds for any $a \geqslant 2$ and p if $(p-1)/2 > 30$, that is, if $p > 61$. For primes $p \leqslant 61$, Lemma 2 can be checked by numerical computation.

For example, in the case $p = 7$ we have $\Phi_3(a) > 3 \cdot 7$ for $a > 4$, and of the numbers $a = 2, 3, 4$ only $a = 2$ and $a = 4$ belong to the exponent $(p-1)/2 = 3$ modulo 7. Or another example: if $p = 37$, then $P = (18) = 3$ and $\Phi_{18}(a) > 37 \cdot 3$ for $a > 2$; however, $a = 2$ does not belong to the exponent 18 modulo 37 since $37 \nmid (2^{18} - 1)$.

LEMMA 3. *Let a, k, and m be positive integers satisfying $a > 1$, $m - k > 1$, and $(a, m) = 1$. Let a belong to the exponent $h(m)$ modulo m. If $h(m) \mid (m-k)$ but $h(m) < m - k$, then congruence* (1) *has infinitely many composite n-solutions, unless $m - k = 2$ and $a + 1$ is a power of* 2, *or $m - k = 6$ and $a = 2$.*

Proof. Let a, k, and m be integers satisfying the conditions of the lemma. $n = m$ satisfies congruence (1) since $h(m) \mid (m - k)$. As it is well known, for any integer $n > 1$ there is a prime q such that a belongs to the exponent $h(q) = n$ modulo q, unless $n = 2$ and $a + 1$ is a power of 2, or $n = 6$ and $a = 2$ (see [1] or [7]). Thus, there exists a prime p for which $h(p) = m - k$. Since $h(m) < h(p) = m - k$ and $h(m) \mid (m - k)$, we have $p \nmid m$ and $h(mp) = m - k$. On the other hand, $h(p) = m - k$ implies that $(m - k) \mid (p - 1)$, and so $mp - k = (m - k)p + k(p - 1)$ is divisible by $h(mp) = m - k$. From this fact it follows that $n = mp$ also satisfies congruence (1), and one can easily see that $mp - k > 2$ if $a > 2$ and $mp - k > 6$ if $a = 2$; furthermore, $h(mp) = m - k < mp - k$. Continuing this process, we get infinitely many solutions of (1).

3. Proof of the Theorem. Let a and k be fixed positive integers. Using the results of Makowski and Rotkiewicz mentioned above, we may assume that

$$(k, a) > 1, \tag{6}$$

$$k \neq 3 \tag{7}$$

and

$$a = 2b \geqslant 4 \quad \text{if } k = 2, \tag{8}$$

where b is an integer.

First let $k = 2$ and so, by (8), $a \geqslant 4$ is an integer of the form $a = 2b$. If $a = 4$ and $m = 7 \cdot 11 = 77$, then $h(7) = 3$, since $7 \mid (4^3 - 1)$ but $7 \nmid (4^i - 1)$ for $i = 1, 2$, and similarly $h(11) = 5$. From this it follows that $h(77) = 15$, and using Lemma 3 with $m = 77$, we get infinitely many solutions of (1).

In the case $k = 2$, $a = 2b > 4$, Lemma 3 with $m = a - 1$ also yields the proof of the Theorem, since in this case $h(m) = 1$ is a divisor of $m - k$ and $h(m) < m - k = a - 3$.

Now let $k \geqslant 4$. As we have seen above, there is a prime p such that $h(p) = k - 1$, since $k - 1 > 2$ and, by (6), $k - 1 \neq 6$ if $a = 2$. For this prime p, Fermat's congruence theorem implies that $p - k = (p - 1) - (k - 1)$ is divisible by $h(p) = k - 1$; furthermore, $p - k \neq 0$ by (6), and so obviously $p - k \geqslant h(p) = k - 1 \geqslant 3$

and $p - k \neq 6$ if $a = 2$. Thus the assertion of the Theorem follows from Lemma 3 with $m = p$ if $p - k \neq h(p) = k - 1$. If $p - k = h(p) = k - 1$ and $h(p) = h(p^2)$, then our assertion can be seen with $m = p^2$ similarly as above, since $p^2 - k = (p^2 - 1) - (k - 1)$ is divisible by $h(p^2) = k - 1$.

Thus, in the sequel we may assume that $k \geqslant 4$ and p is a prime such that $h(p) = k - 1$, $p - k = k - 1$, and $h(p) \neq h(p^2)$.

Let $n \geqslant 2$ be an integer and let $\{p_1, \ldots, p_r\}$ be the set of all primitive prime divisors of $a^n - 1$; i.e., $h(p_i) = n$ for $i = 1, \ldots, r$. If $e_i > 0$ is the greatest integer for which $p_i^{e_i} | (a^n - 1)$, $i = 1, \ldots, r$, then

$$\Phi_n(a) = \lambda \cdot \prod_{i=1}^{r} p_i^{e_i}, \tag{9}$$

where $\lambda = 1$ or $P(n)$ (see, e.g., [1]). Since by our assumption $h(p) = k - 1 = (p - 1)/2 \geqslant 3$ and $h(p) \neq h(p^2)$, Lemma 2 and (9) imply that there is a prime q for which $q \neq p$ and $h(q) = (p - 1)/2 = k - 1$, unless $(p; a)$ is one of the pairs of integers listed in Lemma 2. For this prime, $h(q) | (q - k)$ and $h(q) < q - k$, since otherwise $p = q$ would follow. Using Lemma 3 with $m = q$, the Theorem follows in this case.

If $(p; a)$ is one of the pairs listed in Lemma 2, $k \geqslant 4$ and $p - k = k - 1 = h(p)$, then $k = (p + 1)/2$ and so $(k; a) = (2; 4), (3; 4), (3; 9), (4; 2), (4; 4), (7; 4), (9; 2)$ or $(21; 2)$. Since we have proved the Theorem in the case $k = 2$, by (6) and (7) we have to deal only with the cases $(k; a) = (4; 2)$ and $(4; 4)$.

Using the computer TPA 11-40, we have checked that $n | (a^{n-k} - 1)$ if $n = 40369 = 7 \cdot 73 \cdot 79$ in the case $a = 2$, $k = 4$, and if $n = 19 \cdot 31 = 589$ in the case $a = 4$, $k = 4$. These numbers n are composite, and so $h(n) < n - k$. By Lemma 3, this completes the proof of the Theorem.

We note that in the cases $(k; a) = (4; 2)$ and $(4; 4)$ the number $n = 7$ satisfies congruence (1), but it does not imply infinitely many solutions since the condition $h(m) < m - k$ of Lemma 3 does not hold for $m = 7$. For some pairs $(k; a)$ we give below a table of the least composite integers n which satisfy congruence (1). In some cases, (1) holds for primes less than the numbers given in the table; these cases are $(k; a; n) = (3; 4; 5), (4; 2; 7), (4; 4; 7), (5; 5; 13)$, and $(6; 2; 31)$.

We would like to thank G. Dorkó and A. Láng for their valuable help in the numerical computations.

a \ k	2	3	4	5	6
2	$20737 = 89 \cdot 233$	$9 = 3^2$	$40369 = 7 \cdot 73 \cdot 79$	$25 = 5^2$	$18631 = 31 \cdot 601$
3	$4 = 2^2$	$9299 = 17 \cdot 547$	$8 = 2^3$	$25 = 5^2$	$8 = 2^3$
4	$77 = 7 \cdot 11$	$9 = 3^2$	$589 = 19 \cdot 31$	$15 = 3 \cdot 5$	$9 = 3^2$
5	$4 = 2^2$	$9 = 3^2$	$6 = 2 \cdot 3$	$62 = 2 \cdot 31$	$8 = 2^3$

Department of Mathematics
Teacher's Training College
Leányka u. 4
3301 Eger, Hungary

1. G. D. Birkhoff & H. S. Vandiver, "On the integral divisors of $a^n - b^n$," *Ann. of Math.* (2), v. 5, 1904, pp. 173–180.

2. A. Makowski, "Generalization of Morrow's D numbers," *Simon Stevin*, v. 36, 1962, p. 71.

D. C. MORROW, "Some properties of D numbers," *Amer. Math. Monthly*, v. 58, 1951, pp. 329–330.

4. D. S. MITRINOVIĆ & M. S. POPADIĆ, *Inequalities in Number Theory*, Naucni Podmladak, Univ. of Niš, 1978, 183 pp.

5. A. ROTKIEWICZ, *Pseudoprime Numbers and Their Generalizations*, Student Assoc. of the Faculty of Sci., Univ. of Novi Sad, 1972, 169 pp.

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

7. K. ZSIGMONDY, "Zur Theorie der Potenzreste," *Monatsh. Math.*, v. 3, 1892, pp. 265–284.