COLLOQUIUM MATHEMATICUM

VOL. LIX 1990 FASC. 2

THE EXISTENCE OF SOLUTIONS OF THE GENERALIZED PSEUDOPRIME CONGRUENCE $a^{f(n)} \equiv b^{f(n)} \pmod{n}$

BY

WAYNE L. McDANIEL (ST. LOUIS, MISSOURI)

1. Introduction. Let f be an integer-valued function of the integer n and $|a| > |b| > 0$ with $(a, b) = 1$. The congruence

$$a^{f(n)} \equiv b^{f(n)} \pmod{n} \tag{0}$$

has been shown to have infinitely many solutions n for a very small set of functions f, and, in each case, for restricted values of a and b (see [14], Chapter 4, Section 10). The best known of these functions is, of course, $f(n) = n-1$. Most efforts to solve (0) have, in fact, involved $f(n)$ equal to the general linear function $cn-k$ for selected values of a, b, c and k; we summarize those results in a paragraph below. In this paper, we prove that if f is a polynomial having a rational zero $r = k/c$, and $f(n)$ is positive for n sufficiently large, then (0) has infinitely many solutions except for certain cases where $|c-k| = 1$ or 2.

It should be observed that a proof of the existence of an infinitude of solutions of (0) for any polynomial f establishes the existence of infinitely many *composite* solutions. Indeed, since there exists a polynomial g such that $f(n)^{\bullet} = (n-1)g(n)+f(1)$, any prime solution of (0) divides $a^{f(1)}-b^{f(1)}$, so (0) has a finite number of prime solutions unless f has $r = 1$ as a zero; since $a^{n-1} \equiv b^{n-1} \pmod{n}$ has been shown to have infinitely many composite solutions (Rotkiewicz [12]), the observation holds in all cases.

Let (A) be the statement

(A) $a^{cn-k} \equiv b^{cn-k} \pmod{n}$ *has infinitely many solutions* n.

Interest in solving (0) began with the discovery that the congruence $2^{n-1} \equiv 1 \pmod{n}$ has not only all odd prime integers as solutions, but also certain composite integers (which came to be known as pseudoprimes). Cipolla [3] proved, in 1904, that infinitely many pseudoprimes exist, and, in 1948, Steuerwald [18] established the existence of infinitely many pseudoprimes with respect to a by proving (A) for $a > 0$ and $b = c = k = 1$. For $k \neq 1$,

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

has been investigated by Morrow [8], who established (A) for $b = c = 1$, $k = 3$

and $(a, 3) = 1$, Mąkowski [7], who proved (A) for $b = c = 1$, $k > 1$ and $(a, k) = 1$, and Rotkiewicz, who proved (A) for $b = c = 1$ and $k = 3$ for all $a > 1$ (see [14], Theorem 32) and established several necessary conditions for (A) to be true. More recently, Rotkiewicz proved (A) for $(a, b, c, k) = (2, 1, 1, 2)$ (see [15]). While this paper was being refereed, we learned that Kiss and Phong [6] have proven (A) for $a > 1$, $b = c = 1$ and $k > 1$, and that Phong [10] has independently proven (A) for a, b and k positive integers and $c = 1$, with the exception of (a, b, k) listed in our Corollary 1.

For $c \neq 1$, (A) has been proven for a and b positive, $c = 2$ and $k = 1$ by Rotkiewicz ([14], p. 29); this result is implicit in his theorem that there exist infinitely many even pseudoprimes with respect to a and b.

Although we have restricted a and b in the first sentence of the Introduction, these restrictions are, of course, quite unnecessary, except that neither a nor b can be 0 if the other is not 0, and are included in the interest of simplifying the statements and proofs of the theorems. We will assume, also, that $c > 0$, and $(c, k) = 1$ or $k = 0$, with the observation that the existence of infinitely many solutions with these restrictions implies the existence of infinitely many solutions when they are removed, provided that (for $c < 0$) negative solutions n are allowed.

In addition to our principal result, we shall prove, in Section 6, an analogue of Corollary 1, below, for the congruence $a^{n-k} \equiv -b^{n-k} \pmod{n}$.

CONDITION C. *For* $k \neq 0$,

$$(\pm a, \pm b, |c-k|) \neq (t+1, t, 1) \quad \textit{for } t \geqslant 1 \textit{ and } c > 1,$$

and

$$(\pm a, \pm b, c, k) \neq \begin{cases} (2^u+1, 2^u-1, 3, 5) \textit{ or } (2^u+1, 2^u-1, 1, 3) & \textit{for } u > 1, \\ (2^v \cdot 5+1, 2^v \cdot 5-1, 1, 3) & \textit{for } v > 0, \\ (t+2, t, 2, 3),\ (t+1, t, 1, 2) \textit{ or } (t+3, t, 1, 2) & \textit{for } t > 1. \end{cases}$$

MAIN THEOREM. *Let f be a polynomial with integer coefficients which has a rational zero $r = k/c$ $(c > 0)$.*

(i) *If $f(n) > 0$ for n sufficiently large, $(\pm a, \pm b, k) \neq (t, t-1, 0)$ for $t > 1$, and Condition C is satisfied, then (0) has infinitely many positive solutions n.*

(ii) *If $f(\pm n) > 0$ for n sufficiently large, (0) has infinitely many solutions n if and only if $(\pm a, \pm b, k) \neq (t, t-1, 0)$ for $t > 1$.*

THEOREM 1. *If Condition C is satisfied, (1) has infinitely many solutions. If $k = 0$, (1) has infinitely many solutions if and only if $(\pm a, \pm b) \neq (t, t-1)$ for $t > 1$.*

COROLLARY 1. *The congruence $a^{n-k} \equiv b^{n-k} \pmod{n}$ has infinitely many solutions n if neither (a, b, k) nor $(-a, -b, k)$ is one of the following triples:*

$$(2^u+1, 2^u-1, 3) \quad \textit{for } u \geqslant 2,$$

$$(2^v \cdot 5+1,\ 2^v \cdot 5-1,\ 3) \quad \textit{for } v > 0,$$

$$(t+1,\ t,\ 2),\ (t+3,\ t,\ 2),\ \textit{or } (t,\ t-1,\ 0) \quad \textit{for } t > 1.$$

Setting $b = 1$, we have

COROLLARY 2. *The congruence* $a^{n-k} \equiv 1 \pmod{n}$ *has infinitely many solutions* n *for each pair of integers* a *and* k *if and only if* $(a, k) \neq (2, 0)$.

2. Preliminary results. Our approach involves exploiting the divisibility properties of the cyclotomic polynomial F_m defined by

$$F_m(a, b) = \prod_{d|m} (a^d - b^d)^{\mu(m/d)} \tag{2}$$

or, alternatively, by

$$F_m(a, b) = \prod_{j} (a - \zeta^j b) \quad (1 \leqslant j < m,\ (j, m) = 1), \tag{3}$$

where ζ is a primitive m-th root of unity.

The divisors of $a^m - b^m$ which are prime to $a^d - b^d$ for $d = 1, 2, \ldots, m-1$ are called *primitive divisors* of $a^m - b^m$. Our definition is essentially that of Birkhoff and Vandiver [2] (it should be noted that some authors have restricted the term primitive divisor to mean a *prime* primitive divisor). It is well known that $F_m(a, b) = p_0^c \prod \prod p_i^{a_i}$, where p_0 is the largest prime factor of m, $c = 0$ or 1 and the p_i are the prime primitive divisors of $a^m - b^m$. Sylvester showed that the primitive divisors of $F_m(a, b)$ are of the form $jm + 1$ ([4], Vol. I, p. 384).

The following basic result on primitive divisors was first proved, for $b = 1$, by Bang [1] in 1886 for positive a and b, $(a, b) = 1$, by Zsigmondy [19] in 1892 and by Birkhoff and Vandiver [2] in 1904, and, more recently, by Kanold [5], and Rotkiewicz [13].

Let $E = \{(r, r-1, 1)$ for $r > 1$, $(r, 2^u - r, 2)$ for $r > 2^u - r > 0$, $(2, -1, 3)$, $(2, 1, 6)\}$.

THEOREM Z. $F_m(a, b)$ *has at least one primitive divisor if* $(\pm a, \pm b, m) \notin E$.

We shall use the notation $P(m)$ for the greatest prime factor of m.

The proof of Theorem 1 requires first showing that for almost all triples (a, b, k), $k \geqslant 2$, $a^{k-1} - b^{k-1}$ has a primitive divisor $> 2k-1$. Schinzel [16] proved that $P(a^m - b^m) \geqslant 2m+1$ if the square-free kernel of ab divides m, or equals ± 2, and $m \neq 4$, 6 or 12 when $|ab| = 2$. We begin our discussion of the magnitude of the primitive divisors of $a^m - b^m$ by obtaining a lower bound on $P(a^m - b^m)$ when $(ab, m+1) > 1$.

THEOREM 2. *Let* $(a, b, m) \neq (2, -1, 3)$ *or* $(-2, 1, 3)$. *If* $m > 2$ *and* $(ab, m+1) > 1$, *then*

(i) $P(a^m-b^m) \geqslant 2m+1$, *and*
(ii) *if* $m \equiv 2 \pmod 4$, $P(a^m-b^m) \geqslant 3m+1$.

Proof. The hypothesis is not satisfied if $F_m(a, b) = F_6(\pm 2, \pm 1)$; hence, by Theorem Z, $F_m(a, b)$ has a prime primitive divisor $p = im+1$. Since $p|a^m-b^m$ and $(a, b) = 1$, $p \nmid ab$, so, by hypothesis, $p \neq m+1$. This proves (i). Assume now that $m \equiv 2 \pmod 4$. We see that $F_{m/2}(a, b)$ has a prime primitive divisor $q = j(m/2)+1$, that j is even since $m/2$ is odd, and that $j \neq 2$ since $q|a^m-b^m$ and $(a, b) = 1$ imply that $q \neq m+1$. The primitive divisors of $F_m(a, b)$ do not divide $F_{m/2}(a, b)$, so either p or q is $\geqslant 3m+1$.

COROLLARY. *If* $m > 2$, $m \equiv 2 \pmod 4$ *and* $(ab, m+1) > 1$, *then* a^m-b^m *has a prime divisor greater than* $2m+1$ *of the form* $jm+1$.

LEMMA 1. *Let* $m > 2$.
(i) $F_m(a, b) > (|a|-|b|)^{\varphi(m)}$.
(ii) $F_m(a, b) > |a|^{\varphi(m)} m^{-d(m)/2}$, *where* $d(m)$ *is the number of positive divisors of* m.
(iii) *If* $m = pM$, p *prime and* $M > 1$, *then* $F_m(a, b) > |a|^{(p-2)\varphi(M)}$.
(iv) *If* $m = pM$, p *prime and* $p|M$, *then* $F_m(a, b) > |a|^{p\varphi(M)} M^{-d(M)/2}$.

Proof. Let $A = |a|$ and $B = |b|$. $F_m(a, b)$ is irreducible and of even degree, $\varphi(m)$, and is therefore positive for all triples (a, b, m).
(i) follows immediately from (3).
(ii) Since, for all positive divisors d of m,

$$1 \leqslant \frac{A-(B/A)^{d-1}B}{A-B} = \frac{A^d-B^d}{A^{d-1}(A-B)} \leqslant \frac{A^{d-1}d}{A^{d-1}} = d,$$

we have

$$0 \leqslant \ln \frac{A^d-B^d}{A^{d-1}(A-B)} \leqslant \ln d$$

with equality holding only if $d = 1$. It follows from (2) that

$$\ln F_m(a, b) > \sum_{d|m} \mu\left(\frac{m}{d}\right)(d \ln A) + \sum_{d|m} \mu\left(\frac{m}{d}\right) \ln\left(\frac{A-B}{A}\right) - \sum_{d|m} \ln d.$$

This proves (ii), since

$$\sum \mu(m/d) = 0, \quad \sum \mu(m/d)\, d = \varphi(m) \quad \text{and} \quad \prod_{d|m} d = m^{d(m)/2}.$$

(iii) It is well known that if $m = pM$, then

$$F_m(a, b) = \begin{cases} F_M(a^p, b^p)/F_M(a, b) & \text{if } p \nmid M, \\ F_M(a^p, b^p) & \text{if } p|M. \end{cases}$$

(See [9], p. 158, for a derivation for $b = 1$.) By (i), $F_M(a^p, b^p) > (A^p - B^p)^{\varphi(M)}$, and since $|a - b\zeta^j| \leqslant A + B$, (3) implies $F_M(a, b) < (A+B)^{\varphi(M)}$; hence

$$F_m(a, b) > \left(\frac{A^p - B^p}{A+B}\right)^{\varphi(M)}.$$

Since $(A^p - B^p)/(A+B) \geqslant A^{p-2}$, (iii) follows.

(iv) follows from (ii), since $F_m(a, b) = F_M(a^p, b^p)$.

Estimates for $\varphi(m)$ are readily obtained by observing that if $m = \prod p_i^{a_i}$ and $c < 1$, then

$$\frac{\varphi(m)}{m^c} = \prod \frac{p_i^{a_i - 1}(p_i - 1)}{p_i^{a_i c}} = \prod p_i^{(a_i - 1)(1-c)} \frac{p_i - 1}{p_i^c} \geqslant \prod \frac{p_i - 1}{p_i^c}.$$

If $c \leqslant .86$, then $(p_i - 1)/p^c > 1$ for $p_i \geqslant 5$, and the minimum value of $1/2^c$, $2/3^c$, and $(1/2^c)\cdot(2/3^c)$ is $> .428$. If $c \leqslant .5$, then $(p_i - 1)/p^c > 1$ for $p_i \geqslant 3$, and $(1/2^c)\cdot(2/3^c) > .81$. Thus we have the following lower bounds for $\varphi(m)$:

LEMMA 2. (i) *If* $m \geqslant 2$, *then* $\varphi(m) > .428\, m^{.86}$.

(ii) *If* $m > 2$, *then* $\varphi(m) > .81\, m^{.5}$.

It is clear that, apart from the exceptions given by Theorem Z, $F_m(a, b)$ has a large primitive divisor (not necessarily prime) when m is large and $|a - b| > 1$, since $F_m(a, b)$ exceeds $|a - b|^{\varphi(m)}$ and has no prime divisor greater than m which is not primitive. Lemma 3 below reduces the set of triples (a, b, m) for which $F_m(a, b)$ does not clearly have a primitive divisor greater than $2m+1$ to a manageable size.

Let $r > |t| > 0$ and $(r, t) = 1$. Let

$$S_1 = \{(2, 1, 3), (4, 1, 3), (3, -1, 3), (3, -2, 3), (5, -1, 3), (5, -4, 3),$$
$$(2, -1, 5), (3, -2, 5), (2, \pm 1, 4), (3, \pm 1, 4), (2, \pm 1, 8), (2, -1, 9),$$
$$(2, 1, 10), (3, 2, 10), (2, 1, 20), (2, \pm 1, 12), (2, 1, 18), (3, 1, 18)\},$$

$$S_2 = \{(r, t, 6): r \leqslant 7\},$$

$$S_3 = \{(r, t, 2): |r + t| \leqslant 5 \text{ or } = 2^v \cdot 3 \text{ or } 2^v \cdot 5 \text{ for } v > 0\},$$

$$S_4 = \{(r, t, 1): |r - t| = 2 \text{ or } 3\},$$

$$S = S_1 \cup S_2 \cup S_3 \cup S_4.$$

Let

$$U = \{(r, 2^v \cdot 3 - r, 2) \text{ for } r > 1 \text{ and } v \geqslant 0, (t + c, -t, 2) \text{ for } c = 1, 2, 3$$
or 4 and $t > 0$, $(t+2, t, 1)$ for $t > 0$, $(2, 1, 2)$, $(3, 1, 2)$, $(2, \pm 1, 4)$,
$(3, \pm 1, 4)$, $(2, \pm 1, 6)$, $(3, 1, 6)$, $(3, 2, 6)$, $(4, -1, 6)$, $(5, 1, 6)$, $(5, 4, 6)$,
$(2, 1, 10)$, $(3, 2, 10)$, $(2, \pm 1, 12)$, $(2, 1, 18)\}$.

LEMMA 3. *Let $m \geq 1$, and $F_m(a, b)$ be such that $(\pm a, \pm b, m) \notin E$. Then $F_m(a, b)$ has a primitive divisor greater than $2m+1$ if $(\pm a, \pm b, m) \notin S$, and a primitive divisor greater than $m+1$ iff $(\pm a, \pm b, m) \notin U$.*

Proof. If $m = 1$, $n = |a-b|$ divides $F_m(a, b) = a-b$ and $n > 2m+1$ unless $|a-b| = 2$ or 3. If $m = 2$, $F_m(a, b) = a+b$ clearly has a primitive divisor $> 2m+1 = 5$ unless $(a, b, m) \in S_3$. Assume $m > 2$.

Let p be the largest prime factor of m. If the theorem is not true, then

$$F_m(a, b) = p^c(m+1) \text{ or } p^c(2m+1), \quad \text{where } c = 0 \text{ or } 1.$$

It suffices to show that $F_m(a, b) > p(2m+1)$.

If m is prime, $F_m(a, b) = (a^m - b^m)/(a-b) > |a|^{m-2}$ is greater than $m(2m+1)$ for all a such that $|a| \geq 2$ if $m \geq 11$. Upon computing $F_m(a, b)$ for $m = 3$, 5 and 7 directly, we find that $F_m(a, b)$ has a primitive divisor $> 2m+1$ for m prime unless (a, b, m) or $(-a, -b, m)$ is one of the first eight triples in S.

If m is a power of 2 ($m \geq 4$), $F_m(a, b) = a^{m/2} + b^{m/2}$ is readily seen to have a primitive divisor greater than $2m+1$ except when $(a, b, m) = (2, \pm 1, 4)$, $(3, \pm 1, 4)$ or $(2, \pm 1, 8)$. If m is a power of 3 ($m \geq 9$), then

$$a^m - b^m = \Big[\prod_{d \mid m/3} F_d(a, b)\Big] \cdot F_m(a, b) = (a^{m/3} - b^{m/3}) F_m(a, b)$$

implies that

$$F_m(a, b) = a^{2m/3} + a^{m/3} b^{m/3} + b^{2m/3} > \begin{cases} a^{2m/3} & \text{if } a > 0, \\ (a^{2m/3})/2 & \text{if } a < 0; \end{cases}$$

hence $F_m(a, b) > 3(2m+1)$ unless (a, b, m) or $(-a, -b, m) = (2, -1, 9)$.

Assume now that $m = pM$, $M > 1$, m not a power of 2 or 3. Let

$$f(a, p, M) = |a|^{(p-2)(.81M^{.5})} - p(2pM+1), \tag{4}$$

$$g(a, p, M) = |a|^{(p-2)(.428M^{.86})} - p(2pM+1). \tag{5}$$

When $p \geq 11$ and $|a| \geq 2$, (4) is a positive increasing function of M. By Lemma 1 (iii) and Lemma 2 (ii), then, $F_m(a, b)$ has a primitive divisor $> 2m+1$ if the largest prime factor p of m is ≥ 11.

When $p = 7$, we find similarly that (4) is positive if $M \geq 5$. Now, when $M = 5$ (and $p = 7$), $.81 M^{.5} < 1.82$ and $p(2pM+1) = 497$. So, if $M < 5$ and $\varphi(M) > 1.82$ (i.e., $2 < M < 5$), then

$$F_m(a, b) - 7(14M+1) > 2^{5\varphi(M)} - 7(14M+1) > 2^{5\varphi(M)} - 497 > f(2, 7, 5) > 0.$$

Hence, when $p = 7$, $F_m(a, b)$ has a primitive divisor $> 2m+1$ unless $(|a|, |b|, m) = (2, 1, 14)$. However, $F_{14}(2, 1)$ and $F_{14}(2, -1)$ are divisible by 43 and 127, respectively, primitive divisors $> 2m+1$.

When $p = 5$, (5) holds for $|a| \geq 2$ if $M \geq 10$. Hence, by reasoning as above, the inequality $F_m(a, b) - 5(10M+1) > 0$ fails only if $\varphi(M) < 3.10$, i.e., if $M = 2$,

4 or 6. We find, for these values of M, that $a^{3\varphi(M)}-5(10M+1)>0$ unless $(|a|, |b|, m) = (2, 1, 10)$, $(2, 1, 20)$, $(2, 1, 30)$, $(3, 1, 10)$, $(3, 2, 10)$, $(4, 1, 10)$ or $(4, 3, 10)$. Corresponding to these triples, $F_m(a, b)$ has a divisor $> 2m+1$ except when $(\pm a, \pm b, m) = (2, 1, 10)$, $(3, 2, 10)$ or $(2, 1, 20)$.

When $p = 3$, (5) is positive for all a if $M \geqslant 37$, which implies, as above, that $F_m(a, b)-3(6M+1)$ is positive only if $\varphi(M) > 9.6$. We find, since p is the largest prime factor of $m = pM$, and M is not a power of 3, that $F_m(a, b)$ has a primitive divisor $> 2m+1$ except when $m = 6$, 12, 18, 24, 36, 48, 54 or 72. Now, for these values of m,

$$F_m(a, b) = \frac{a^{m/2}+b^{m/2}}{a^{m/2p}+b^{m/2p}} > \frac{a^{m/2}}{2a^{m/2p}} \geqslant 2^{(m/2-m/2p-1)}$$

which exceeds $3(2m+1)$ for $m = 36$, 48, 54 and 72.

By direct computation, $F_6(a, b) = a^2-ab+b^2 > 3(2\cdot 6+1)$ if $|a| \geqslant 8$. We now examine $F_m(a, b)$ for $p = 3$, $m \neq 6$, using Lemma 1 (iv). Since $p|M$ implies that $F_m(a, b) = F_M(a^p, b^p)$, Lemma 1 (iv) implies that $F_m(a, b) > 3(2m+1)$ if

$$|a|^{p\varphi(M)} > M^{d(M)/2}\cdot 3(6M+1). \tag{6}$$

If, for example, $m = 18$, we have $p = 3$, $M = 6$, $\varphi(M) = 2$, $d(M) = 4$, so (6) implies that $|a| > 3.99$. If (6) is evaluated similarly, but taking $p = 2$ for $m = 12$ and 24, we find that $F_m(a, b)$ has a primitive divisor $> 2m+1$ for $(|a|, m) = (|a| > 7, 6)$, $(|a| > 6, 12)$, $(|a| > 3, 18)$, and $(|a| > 4, 24)$. Applying Lemma 1 (i), with $m = 12$, 18 and 24, we obtain $|a|-|b| \leqslant 2.94$, 2.19 and 1.86, respectively. Upon computing $F_m(a, b)$ for $m = 6$, 12, 18 and 24, for a and b satisfying these conditions, we find that if 3 is the largest prime factor of m, $F_m(a, b)$ has a primitive divisor greater than $2m+1$ unless (a, b, m) or $(-a, -b, m)$ is $(2, \pm 1, 12)$ or $(2, 1, 18)$, or is in S_2.

An examination of $F_m(a, b)$ for $(\pm a, \pm b, m)$ in S reveals that $F_m(a, b)$ has a primitive divisor $> m+1$ unless $(\pm a, \pm b, m)$ is in the set U. This completes the proof.

3. The congruence $a^{cn-k} \equiv b^{cn-k} \pmod n$. We showed in the last section that, with certain exceptions, $F_m(a, b)$ has a primitive divisor $> 2m+1$. In this section, we prove a generalization (Theorem 3) of a theorem due to Mąkowski [7] which will enable us to prove Theorem 1 for "most" of the quadruples (a, b, c, k) for which $c = 1$ and $F_{k-1}(a, b)$ does not have a primitive divisor $> 2k-1$. We next observe that each primitive divisor n of $F_{|c-k|}(a, b)$ is a solution of (1); the existence of infinitely many solutions of (1) when

$$n > (2k-1)/(2c-1) \quad \text{and} \quad n \neq (k-1)/(c-1)$$

then follows from Theorem 6. We prove also that (1) holds for $k \leqslant 0$ if and only if $(\pm a, \pm b, k) \neq (t, t-1, 0)$.

THEOREM 3. *If $k \geqslant 2$ and $(ab, k) = 1$, then there exist infinitely many integers n satisfying the congruence $a^{n-k} \equiv b^{n-k} \pmod n$.*

Proof. Let $k = \prod p_i^{a_i}$, p_i distinct primes, let $m = \prod p_i$, and let

$$t > \max\{|a|, |b|, k, 6\}.$$

By Theorem Z, there exists a prime divisor p of $F_{t\varphi(m)}(a, b)$ of the form $p = jt\varphi(m)+1$. Now

$$kp-k = k(p-1) = kjt\varphi(m) = \varphi(k)mjt.$$

Hence $a^{kp-k}-b^{kp-k}$ is divisible by both p and k; since $(p, k) = 1$, $n = pk$ is a solution of $a^{n-k} \equiv b^{n-k} \pmod{n}$.

THEOREM 4. *If* $n|(a^{|c-k|}-b^{|c-k|})$, *and* $n = j|c-k|+1$ *for some integer* $j \geqslant 1$, *then* n *satisfies* (1).

Proof. We have

$$cn-k = c(j|c-k|+1)-k = |c-k|\left(cj+\frac{c-k}{|c-k|}\right) \geqslant 0.$$

Since the primitive divisors of $F_{|c-k|}(a, b)$ are of the form $j|c-k|+1$, we have immediately the following

COROLLARY. *Every primitive divisor of* $F_{|c-k|}(a, b)$ *is a solution of* (1).

THEOREM 5. *If* $k \leqslant 0$, (1) *has infinitely many solutions iff* $(\pm a, \pm b, k) \neq (t, t-1, 0)$ *for* $t > 1$.

Proof. Assume $k \leqslant -1$. $F_{c-k}(a, b)$ has a primitive divisor except when $(\pm a, \pm b, c-k)$ is one of the last three of the four triples in the set E preceding Theorem Z. Corresponding to these triples, (1) has the solution $n = |2a-2^u|$, 3, and 7, respectively. Assume now that $F_{c-k}(a, b)$ has a primitive divisor N. By the Corollary to Theorem 4, N is a solution of (1). Rotkiewicz's Theorem 34 ([14], p. 130) proves that, for $a > b \geqslant 1$, $a^{f(n)} \equiv b^{f(n)} \pmod{n}$ has infinitely many solutions for certain functions $f(n)$ (including all polynomials with integer coefficients) provided there exists a solution n_0 such that $2 < f(n_0) \geqslant n_0$ and $f(n) > n/2$ for all $n > n_0$. The theorem is readily extended to all a, b such that $|a| > |b| > 0$, and when $f(n) = cn-k$ and n_0 is any positive integer, the hypothesis of the extended theorem is satisfied. That is, (1) has infinitely many solutions if $k \leqslant -1$.

Assume $k = 0$. Since every solution of $a^n \equiv b^n \pmod{n}$ is a solution of $a^{cn} \equiv b^{cn} \pmod{n}$, we may assume $c = 1$. Rotkiewicz has observed ([14], p. 131) that it follows from his Theorem 34 that if $a-b > 1$, then $a^n \equiv b^n \pmod{n}$ has infinitely many solutions, and it is clear from the theorem extended to $|a| > |b| > 0$ that infinitely many solutions exist if $|a-b| > 1$. Suppose that $|a-b| = 1$, that $n = N$ is a solution of $a^n \equiv b^n \pmod{n}$, and that p is the least prime factor of N. Let $N = pm$ and s be the least exponent such that $a^s \equiv b^s \pmod{p}$. Since $a^{pm} \equiv b^{pm} \pmod{p}$, we have $a^m \equiv b^m \pmod{p}$, im-

plying that $s|m$. But $s|p-1$, which implies that $s \leqslant p-1 < p$. This is possible only if $s = 1$, since m has no prime divisors less than p; hence $p|a-b$, an impossibility. This completes the proof.

Rotkiewicz has shown, for $a > b \geqslant 1$, that if $f(n)$ satisfies a certain set of conditions, the congruence $a^{f(n)} \equiv b^{f(n)} \pmod{n}$ has infinitely many solutions provided there exists a single composite solution n_0 such that $2 < f(n_0) \geqslant n_0/2$ and $f(n) \geqslant n/4$ for $n > n_0$ ([14], Theorem 31). We show, in the following theorem, that the conclusion holds, for $|a| > |b| > 0$, whether n_0 is composite or prime if $f(n) = cn-k$, subject to the condition that

$$1 < n > (2k-1)/(2c-1) \quad \text{and} \quad n \neq (k-1)/(c-1).$$

THEOREM 6. *If there exists a solution $n > (2k-1)/(2c-1)$ of (1), such that $n > 1$ and $n \neq (k-1)/(c-1)$, then the congruence has infinitely many composite solutions.*

Proof. Since there exist infinitely many pseudoprimes with respect to a and b, the theorem is true when $c = k = 1$ and is true when $k \leqslant 0$ by Theorem 5 (independent of the hypothesis).

Assume that $ck \neq 1$ and $k > 0$. Suppose (1) has at least one solution satisfying the hypothesis of the theorem, but only finitely many solutions (as noted in the Introduction, (1) has only a finite number of prime solutions), and let N denote the largest solution. We show that Theorem Z (with $m = cN-k$) assures the existence of a prime q such that qN is also a solution.

Suppose, first, that $(\pm a, \pm b, |c-k|)$ is in E. We observe that $F_{cN-k}(a, b) \neq F_{|c-k|}(a, b)$. If $c = 1$, $cN-k = |c-k|$ implies that $N = 1$ or $N = 2k-1$, neither of which is possible. Assume that $c > 1$. If $cN-k = |c-k| = 2$, 3 or 6, then (since $(c, k) = 1$ and $c > 0$) we have $c = 2$ and $k = 5$ for $|c-k| = 3$; but then $N = 4$, which is impossible since $(\pm 2)^{2n-5} \equiv (\mp 1)^{2n-5} \pmod{n}$ has no even solutions.

By Theorem Z, then, $F_{cN-k}(a, b)$ has a divisor $q = j(cN-k)+1$, $j \geqslant 1$. Since

$$N > (2k-1)/(2c-1),$$

we have $q \geqslant j(N/2)+1$. Note now that $(q, N) = 1$. This is obviously true for $j \geqslant 2$, since then $q > N$; if $j = 1$, $q > N/2$, and since neither $ck = 1$ nor $N = (k-1)/(c-1)$ holds, $q \neq N$; so, in this case, too, $(q, N) = 1$. It follows that since $a^{cN-k} - b^{cN-k}$ is divisible by both q and N, $a^{cN-k} \equiv b^{cN-k} \pmod{qN}$. Now,

$$c(qN)-k = c[j(cN-k)+1]N-k = (cN-k)(cjN+1),$$

and therefore (1) holds with $n = qN$. This proves the theorem.

4. Proof of Theorem 1. It suffices to prove the theorem for (a, b, c, k) with a positive, since each solution of $a^{cn-k} \equiv b^{cn-k} \pmod{n}$ is a solution of $(-a)^{cn-k} \equiv (-b)^{cn-k} \pmod{n}$.

We may assume that $k > 0$, since Theorem 5 proved Theorem 1 for $k \leqslant 0$. If $c > 1$, it is easy to show that if $N = j|c-k|+1$ and $(j, c) \neq (1, 2)$, then

$$N > (2k-1)/(2c-1) \quad \text{and} \quad N \neq (k-1)/(c-1).$$

Since, by the Corollary to Theorem 4, each primitive divisor of $F_{|c-k|}(a, b)$ is a solution of (1), it follows from Theorem 6 that the theorem is true for $c > 2$ unless $(\pm a, \pm b, |c-k|)$ is in E. Checking the elements of E, we find that $N = 3$, $N = 7$ and $N = |2a-2^u|$ are solutions of (1) for $(\pm a, \pm b, |c-k|) = (2, -1, 3)$, $(2, 1, 6)$, and $(a, 2^u-a, 2)$, respectively, with

$$N > (k-1)/(c-1) > (2k-1)/(2c-1)$$

except when $(\pm a, \pm b, c, k) = (2^u+1, 2^u-1, 3, 5)$; in this latter case, when $u = 1$, $N = 5 \cdot 11$ is a solution. By Theorem 6, then, the theorem is proved for $c > 2$. For $c = 2$, we find, similarly, that the theorem is true for (a, b, c, k) if $F_{|c-k|}(a, b)$ has a primitive divisor $> |c-k|+1$. However, examining the set U preceding Lemma 3 and noting that $c = 2$ and $(c, k) = 1$ imply that $|c-k|$ is odd, we see that if $F_{|c-k|}(a, b)$ has a primitive divisor, then it has a primitive divisor $> |c-k|+1$ unless $(\pm a, \pm b, |c-k|) = (t+2, t, 1)$ for $t > 0$. It follows that, since $|c-k|$ is odd, the only possible (a, b, c, k) for which (1) does not have solutions are those excluded in the statement of the theorem, and, corresponding to $|c-k| = 3$, $(2, -1, 2, 5)$ and $(-2, 1, 2, 5)$; however, we find that $n = 139 \cdot 5419$ is a solution of (1) for these latter two quadruples.

Let $c = 1$. If $k = 1$, the theorem is true; assume that $k \geqslant 2$ and let $m = k-1$. We first examine (1) for (a, b, k) such that $F_m(a, b)$ has no primitive divisors. We have previously noted [15] that $2^{n-2} \equiv 1 \pmod{n}$ has infinitely many solutions, proving the theorem when $b = 1$ and $|a-b| = 1$. By Lemma 3, the Corollary to Theorem 4, and Theorem 6, the theorem is true for $(\pm a, \pm b, k) \neq (a, 2^{u+1}-a, 3)$ for $u > 0$, $(2, -1, 4)$, and $(2, 1, 7)$, if $(\pm a, \pm b, m) \notin S$. Now, the theorem holds for $(a, b, k) = (2, 1, 7)$ by Theorem 3, and $n = 3 \cdot 43 \cdot 251$ is a solution of (1) for $(a, b, k) = (2, -1, 4)$. For $(\pm a, \pm b, k) = (a, 2^{u+1}-a, 3)$ with $u \geqslant 0$, we note that, for a positive, $n = |a-b|$ is a solution of (1) with $n \geqslant 2k-1$ unless $a = \pm(2^u+1)$ and $b = \pm(2^u-1)$; we observe that $u \neq 0$, since $(a, b) = 1$, and if $u = 1$, the theorem is true ($b = 1$, $k = 3$; [14], Theorem 32).

Examining the elements of S_4, first, we see that if $|a-b| = 2$, $(a, b) = 1$ implies ab is odd, so infinitely many solutions exist by Theorem 3. If $|a-b| = 3$ and $b = 1$, i.e., $(\pm a, \pm b, k) = (2, -1, 2)$ or $(4, 1, 2)$, $n = 3 \cdot 59 \cdot 4051$ satisfies $2^{n-3} \equiv (-1)^{n-3} \pmod{n}$ and each solution of $2^{n-2} \equiv 1 \pmod{n}$ (see the preceding paragraph) satisfies $4^{n-2} \equiv 1 \pmod{n}$.

Examining the elements of S_3, now, we observe that if $|a+b| = 2^v \cdot 5$ (i.e., $(\pm a, \pm b, k) = (a, 2^{v+1} \cdot 5-a, 3)$), $n = |a-b| = |2a-2^{v+1} \cdot 5|$ is a solution of (1) with $n > 2k-1$ unless $(a, b, k) = (2^v \cdot 5+1, 2^v \cdot 5-1, 3)$ (since $(a, b) = 1$, $v \geqslant 1$) or $(7, 3, 3)$, and (1) holds for $(7, 3, 3)$ if $n = 11 \cdot 73$. If $|a+b| \leqslant 5$, it is clear that

$n = |a-b|$ is again a solution unless $|a-b| \leqslant 5$, i.e., unless (a, b, k) or $(-a, -b, k) = (2, \pm 1, 3), (4, \pm 1, 3), (3, \pm 1, 3)$ or $(3, \pm 2, 3)$. Now the theorem is true for the first two of these four triples, and, also for $(a, 2^v \cdot 3 - a, 3)$ $(v \geqslant 1)$ by Theorem 3. The theorem is true for the latter two triples by Rotkiewicz's Theorem 32 ($b = 1$, $k = 3$; [14]) which is readily seen to hold also for $b = -1$ when $a < 9$.

The theorem is true as well for those triples (a, b, k) such that $|a| = 7$ and $m = 6$, by the Corollary to Theorem 2, Theorems 4 and 6. The congruence $a^{n-k} \equiv b^{n-k} \pmod{n}$ has the solution

$$n = 127 \cdot 13\,367$$

for (a, b, k) equal to both $(2, 1, 4)$ and $(4, 1, 4)$, and

$$n = 463 \cdot 7039,\ 9,\ 513\,101 \cdot 28\,909\,244\,547\,481,\ 3 \cdot 19 \cdot 43\,691 \text{ and } 3 \cdot 43$$

are solutions for $(a, b, k) = (3, -2, 4)$, $(5, -4, 4)$, $(3, -2, 6)$, $(2, -1, 6)$ and $(2, -1, 10)$, respectively, eliminating $(a, b, m) = (2, 1, 3)$, $(4, 1, 3)$, $(3, -2, 3)$, $(5, -4, 3)$, $(3, -2, 5)$, $(2, -1, 5)$ and $(2, -1, 9)$ in S_1. The remaining triples $(a, b, m) = (a, b, k-1)$ in S have the property that $(ab, k) = 1$; applying Theorem 3 completes the proof of Theorem 1.

5. Proof of the Main Theorem. The existence of the rational zero $r = k/c$ implies that, for some polynomial g, $f(n) = (cn-k)g(n)$, and, by Theorem 1, that $a^{cn-k} \equiv b^{cn-k} \pmod{n}$ has infinitely many solutions if the hypothesis of (i) of the Main Theorem is satisfied. Thus, if there exists an integer n_0 such that $f(n) > 0$ for $n > n_0$, all solutions $N > n_0$ of $a^{cn-k} \equiv b^{cn-k} \pmod{n}$ are solutions of (0), proving (i).

Assume now that there exists an integer n_1 such that $f(\pm n) > 0$ if $n > n_1$. We let $N > n_1$ and observe that

$$N \mid (a^{cN-k} - b^{cN-k}) \quad \text{iff} \quad -N \mid (a^{-c(-N)-k} - b^{-c(-N)-k}).$$

Since $f(n) = (cn-k)g(n) = (-c(-n)-k)g(n)$, part (i) implies that (0) has infinitely many solutions unless $|c-k| = 1$ or 2, and $|-c-k| = 1$ or 2, proving (ii) for $k \neq 0$. But when $k = 0$, it is immediate from Theorem 1 that (0) has infinitely many solutions iff $(\pm a, \pm b) \neq (t, t-1)$, completing the proof.

6. Related results and comments. In [14], p. 132, Rotkiewicz proves the following theorem:

THEOREM R. *Let f be a function such that if $p \nmid n$ and $p \equiv 1 \pmod{f(n)}$, then $f(n) \mid f(np)$. If $f(n)$ and $f(np)$ are divisible by the same power of 2 and n_0 is a solution of*

$$a^{f(n)} + b^{f(n)} \equiv 0 \pmod{n}, \tag{6}$$

with the properties that $(a, b, f(n_0), n_0) \neq (2, 1, 3, 3)$, $1 < f(n_0) \geqslant n_0/2$ and $f(n) > n/4$ for $n > n_0$, then (6) has infinitely many composite solutions.

Although the theorem is proved for $a > b \geqslant 1$, it is readily seen to hold for $|a| > |b| \geqslant 1$, provided we require, additionally, that $(a, b, f(n_0), n_0) \neq (-2, -1, 3, 3)$.

A result similar to the Main Theorem can be proved for the congruence $a^{f(n)} \equiv -b^{f(n)} \pmod{n}$; because the details are similar and because partial results exist in the literature for $f(n)$ equal to $n-k$, we prove only the following theorem:

THEOREM 7. *The congruence*

$$a^{n-k} \equiv -b^{n-k} \pmod{n} \tag{7}$$

has infinitely many solutions except, possibly, when $(\pm a, \pm b, k) = (r, 2^u - r, 2)$ *for* $r > 2^u - r > 0$, $(r, 2^v \cdot 3 - r, 2)$ *for* $r > 1$ *and* $v \geqslant 0$, $(t+c, -t, 2)$ *for* $c = 1, 2, 3$ *or* 4 *and* $t > 0$, *or* $(r, t, 1)$ *for* rt *even.*

Proof. As in the proof of Theorem 1, it is sufficient to prove the theorem for positive values of a.

Let $k \leqslant 0$. Assume that $(\pm a, \pm b, k) \neq (r, 2^u - r, 0)$ for $r > 2^u - r > 0$, or $(2, 1, -2)$. Then $F_{2-2k}(a, b)$ has a primitive divisor N by Theorem Z; N divides $a^{2-2k} - b^{2-2k}$ and therefore divides $a^{1-k} + b^{1-k}$. Since

$$N - k = j(2-2k) + 1 - k = (1-k)(2j+1)$$

for some integer j, N divides $a^{N-k} + b^{N-k}$. Assuming now that $(\pm a, \pm b, k) = (r, 2^u - r, 0)$ or $(2, 1, -2)$, we see that $N | a^{N-k} + b^{N-k}$ for $N = 2$ in the former case and for $N = 7$ in the latter. Hence (7) holds for all triples (a, b, k), by Theorem R with $f(n) = n - k$ and $n_0 = N$.

Let $k \geqslant 1$. If $k = 1$, and $a+b$ is even, $N = 2$ satisfies (7). Assume now that $k \geqslant 2$ and that $(\pm a, \pm b, k) \neq (r, 2^u - r, 2)$ for $r > 2^u - r > 0$, or $(2, 1, 4)$. Then $F_{2k-2}(a, b)$ has a primitive divisor N, and, as in the case $k \leqslant 0$, the theorem is true by Theorem R with $f(n) = n - k$ and $n_0 = N$ provided $N - k \geqslant N/4$, i.e., $N > 2k - 1$. Let $m = 2k - 2$. Since $N = j(2k-2) + 1$, this implies that the theorem is true if $F_m(a, b)$ has a primitive divisor $> m+1$, that is, $F_m(a, b) \notin U$. Eliminating the triples $(a, b, m) = (r, 2^v \cdot 3 - r, 2)$ and $(t+c, -t, 2)$ from U, we see that the theorem is true if it is true for $(a, b, k) = (2, 1, 2)$, $(3, 1, 2)$, $(2, \pm 1, 3)$, $(3, \pm 1, 3)$, $(2, -1, 4)$, $(3, 1, 4)$, $(3, 2, 4)$, $(4, -1, 4)$, $(5, 1, 4)$, $(5, 4, 4)$, $(2, 1, 6)$, $(3, 2, 6)$, $(2, \pm 1, 7)$, $(2, 1, 10)$ and for the triple $(2, 1, 4)$ excluded above. Now if $(a, b, k) = (2, 1, 2)$, $(2, -1, 4)$, $(3, 2, 4)$, $(4, -1, 4)$, $(5, 4, 4)$, $(2, 1, 6)$, $(3, 2, 6)$, $(2, 1, 10)$ or $(2, 1, 4)$, $a^{n-k} \equiv (-b)^{n-k} \pmod{n}$ has been shown in the proof of Theorem 1 to have infinitely many odd solutions N; since $N - k$ is odd, each solution satisfies (7). By direct computation, we find that, as (a, b, k) ranges through the remaining six triples, $(3, 1, 2)$, $(2, \pm 1, 3)$, $(3, \pm 1, 3)$, $(3, 1, 4)$, $(5, 1, 4)$ and $(2, \pm 1, 7)$, the following integers are, respectively, solutions of (7):

$$N = 61 \cdot 3187,\ 29 \cdot 157,\ 1181 \cdot 5\,301\,533,\ 19 \cdot 31,\ 3 \cdot 23 \cdot 38\,923,\ 37 \cdot 61.$$

Applying Theorem R with $f(n) = n - k$ and $n_0 = N$ completes the proof.

Rotkiewicz observed that it follows immediately from Theorem R that there exist infinitely many composite integers n such that $n|a^n+1$, a result previously proved by Sierpiński [17], and that if $2\nmid a+b$, there exist infinitely many solutions of $a^n+b^n \equiv 0 \pmod{n}$. These result are extended in the following corollary:

COROLLARY 1. *There exist infinitely many integers n such that* $n|a^n+b^n$.

COROLLARY 2. *The congruence* $a^{n-k}+1 \equiv 0 \pmod{n}$ *has infinitely many solutions n except, possibly, for* $(a, k) = (\pm 2^u-1, 2)$ *for* $u > 1$, $(\pm 2^v \cdot 3-1, 2)$ *for* $v > 0$, *or* $(a, 1)$ *for a even.*

Proof. By the theorem, Corollary 2 is true if $(a, b, k) \neq (2, -1, 2)$, $(3, -1, 2)$, $(4, -1, 2)$ or $(5, -1, 2)$. The integers $n = 89 \cdot 233$, $11 \cdot 757$, $89 \cdot 233$ and $31 \cdot 59$ satisfy (7) for these triples, respectively.

In order to prove Theorems 1 and 7, and the above corollary, it was necessary to find a solution of (1) or (7) for fifteen triples (a, b, k). The calculation was readily carried out on a hand-held Casio fx-4000P programmable calculator with the aid of the following theorem, which is similar to a known result for pseudoprimes. The assignment of successively larger odd integer values $\leqslant 25$ to e_1 yielded a solution of (1) or (7) for each of the fifteen triples.

THEOREM 8. *Let* $n = p_1 p_2 \ldots p_s$. *If* e_i *is the least exponent such that* $a^{e_i} \equiv b^{e_i} \pmod{p_i}$, *then* (1) *holds iff* $e_i | cn/p_i - k$ *for* $i = 1, 2, \ldots, s$.

Proof. (1) holds iff $e_i | cn-k$, but $cn-k = (cn/p_i)(p_i-1)+(cn/p_i-k)$.

Whether the Main Theorem (and Theorem 1) can be proved for the exceptional cases is not clear. It is rather easy to show that the theorem does hold for infinitely many quadruples (a, b, c, k) of each of the excluded forms, but the proof for all quadruples of any one of the forms would appear to be difficult.

REFERENCES

[1] A. S. Bang, *Taltheoretiske undersogelser*, Tidsskrift for Mat. (5) 4 (1886), pp. 70–80 and 130–137.

[2] G. D. Birkhoff and H. S. Vandiver, *On the integral divisors of* a^n-b^n, Ann. of Math. (2) 5 (1904), pp. 173–180.

[3] M. Cipolla, *Sui numeri compositi P, che verificiano la congruenza di Fermat* $a^{P-1} \equiv 1 \pmod{P}$, Ann. Mat. Pura Appl. (3) 9 (1904), pp. 139–160.

[4] L. E. Dickson, *History of the Theory of Numbers*, Chelsea, New York 1952.

[5] H. J. Kanold, *Sätze über Kreisteilungspolynome und ihre Anwendungen auf einige zahlentheoretische Probleme*, J. Reine Angew. Math. 187 (1950), pp. 169–182.

[6] P. Kiss and B. M. Phong, *On a problem of A. Rotkiewicz*. Math. Comp. 48 (1987), pp. 751–755.

[7] A. Mąkowski, *Generalization of Morrow's D numbers*, Simon Stevin 36 (1962), p. 71.

[8] D. C. Morrow, *Some properties of D numbers*, Amer. Math. Monthly 58 (1951), pp. 329–330.

[9] T. Nagell, *Introduction to Number Theory*, Wiley, New York 1951.
[10] B. M. Phong, *Generalized solution of Rotkiewicz's problem*, Mat. Lapok (to appear).
[11] H. Riesel, *Prime Numbers and Computer Methods for Factorization*, Birkhäuser, Boston 1985.
[12] A. Rotkiewicz, *Sur les nombres composés n qui divisent* $a^{n-1}-b^{n-1}$, Rend. Circ. Mat. Palermo (2) 8 (1959), pp. 115–116.
[13] — *Elementary proof of the existence of a prime divisor of* a^n-b^n (in Polish), Prace. Mat. 4 (1960), pp. 21–28.
[14] — *Pseudoprime Numbers and Their Generalizations*, Student Association of the Faculty of Sciences, University of Novi Sad, 1972.
[15] — *On the congruence* $2^{n-2} \equiv 1 \pmod{n}$, Math. Comp. 43 (1984), pp. 271–272.
[16] A. Schinzel, *On primitive prime factors of* a^n-b^n, Proc. Cambridge Philos. Soc. 58 (1962), pp. 555–562.
[17] W. Sierpiński, *Sur les nombres* a^n+1, Elem. Math. 19 (1964), p. 136.
[18] R. Steuerwald, *Über die Kongruenz* $a^{n-1} \equiv 1 \pmod{n}$, Bayer. Akad. Wiss. Math.-Natur. Kl. Sitzungsber. (1948), pp. 69–70.
[19] K. Zsigmondy, *Zur Theorie der Potenzreste*, Monatsh. Math. 3 (1892), pp. 265–284.

DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE
UNIVERSITY OF MISSOURI-ST. LOUIS
ST. LOUIS
MISSOURI 63121, U.S.A.

Reçu par la Rédaction le 13.6.1988