PACIFIC JOURNAL OF MATHEMATICS
Vol 118, No 2, 1985

# EQUATIONS IN PRIME POWERS

D. ESTES, R. GURALNICK, M. SCHACHER AND E. STRAUS(*)

**Equations of form $p^a = (q^n - 1)/(q - 1)$ are considered where $p$ is prime, $q$ a prime power, and $n \geq 3$. These equations occur in group theory and in number theory in an attempt to construct algebraic number fields which are arithmetically equivalent but not isomorphic. Algorithms are sought to determine all solutions when $p$ is fixed.**

Suppose $p$ and $r$ are positive prime integers. In this note we are concerned with solutions

$$p^a = \frac{q^n - 1}{q - 1} \tag{1}$$

where $a$, $q = r^b$, $n$ are positive integers, $n \geq 3$. We will write (1′) for the resulting equation when $q$ is an arbitrary integer that is not necessarily a prime power.

Solutions of (1) have proved to be of interest in classifying finite groups having non-conjugate subgroups which induce the same permutation representation, and the associated problem of finding non-isomorphic number fields with the same Dedekind-zeta function (see for instance [**3**], [**5**], and [**9**]). When (1) has no solution for a given prime $p$, then any two $p$-complements in a finite group are conjugate ([**5**, Corollary 3.2]).

The equations

$$73 = (8^3 - 1/8 - 1) \quad \text{and} \quad 1772893 = (11^9 - 1)/(11^3 - 1)$$

show that solutions of (1) can occur when $q$ is not itself prime. The equation $11^2 = (3^5 - 1)/(3 - 1)$ gives the only known solution of (1) when $a \geq 2$; by [**7**] it is the only solution when $a = 2$. It is proved more generally in [**7**] that the only solution of $y^2 = (x^n - 1)/(x - 1)$ in integers occur when $n = 4$, $x = 7$ or $n = 5$, $x = 3$. One of our results (Theorem 1) shows that in any solution of (1), $n$ is prime and does not divide $a$. The case $a = 3$ had been settled by Nagel [**8**] and Ljunggren [**6**].

---

(*) Our colleague Ernst Straus passed away during the preparation of this paper, and so it could not reflect the careful attention he would have given it. We dedicate this paper to his memory. Ernst Straus had been supported in part by NSF grant MCS-82-03347.

Since [**8**] is so inaccessible, we include a somewhat different version of the proof (Theorem 2).

Baker's estimates on linear combinations of logarithms allows one to give finiteness conditions on solutions to (1′) (cf [**1**]). We close with a discussion of this and some consequences to simple groups.

We would like to thank H. Edgar, D. Shapiro, and A. Van der Poorten for informing us of certain results in the literature.

We will write $(\alpha, \beta)$ for the greatest common divisor of two integers $\alpha$ and $\beta$; this notation will persist with the usual ambiguity up to units when $\alpha$ and $\beta$ are in a principal ideal domain. We write $O_K$ for the integers of a number field $K$. If $\alpha \in K$, we write $N(\alpha)$ for the norm from $K$ to $Q$ of $\alpha$, $Q$ = rational numbers.

Suppose $p$ is a prime. We denote by $v_p$ the additive $p$-adic valuation associated to $p$, i.e. $v_p(m) = a$ if $n = p^a t$, $(t, p) = 1$. The following is an easy application of the little Fermat theorem and the binomial theorem; we omit the proof.

REMARK 1. For any integer $q$ we have

(i) $$v_p(q-1) = 0 \Rightarrow v_p(q^p - 1) = 0$$

(ii) $$v_p(q-1) > 0 \Rightarrow v_p(q^p - 1) = v_p(q-1) + 1 \quad \text{for } p > 2.$$

As a consequence of Remark 1, $(q^p - 1)/(q - 1)$ is never divisible by $p^2$ for $p \neq 2$; this is the form in which we usually use Remark 1.

LEMMA 1. *In any solution of* (1′) *we have*:

(i) $n$ *is prime.*

(ii) *if* $q = r^m$, *then* $m = n^e$ *and* $p = 1 \pmod{n^{e+1}}$.

(iii) $p \neq 2$.

(iv) $p$ *is not a Fermat prime.*

*Proof.* Suppose $n = \alpha\beta$ with $1 < \alpha, \beta$. Then

$$p^a = \frac{q^n - 1}{q - 1} = \frac{q^{\alpha\beta} - 1}{q^\alpha - 1} \cdot \frac{q^\alpha - 1}{q - 1}. \tag{2}$$

Hence $q^\alpha \equiv 1 \pmod{p}$ and so $(q^{\alpha\beta} - 1)/(q^\alpha - 1) \equiv \beta \pmod{p}$. Thus $p \mid \beta$. Since this holds for an arbitrary divisor of $n$, it follows that either $n$ is prime or $n$ is a power of $p$.

First assume $p = 2$. If $n$ is a power of 2, then (as $n > 2$) by (2) we have

$$(q^4 - 1)/(q - 1) = (q^2 + 1)(q + 1) = 2^b.$$

However, $q^2 + 1 \neq 0 \pmod 4$ and $q \neq 1$, so this cannot hold. If $n$ is prime, then $(q^n - 1)/(q - 1)$ is odd. Thus (ii) holds.

We can assume now $p > 2$. If $n$ is not prime, then by (2) and what was derived above

$$\frac{q^p - 1}{q - 1} = p^b.$$

As $p^2 \nmid (q^p - 1)/(q - 1)$ by Remark 1, $b = 1$. But then $q \equiv 1 \pmod p$ and $p \equiv 1 \pmod q$, and so $q = -(p - 1)$, a contradiction. Thus (1) holds and $n \neq p$.

Next assume $q = r^m$. To prove the first part of (ii), it suffices to show that if $m$ is prime then $m = n$. If not, then

$$p^a = \frac{r^{mn} - 1}{r^m - 1} = \phi_{mn}(r)\phi_n(r) \tag{3}$$

where $\phi_d(x)$ is the $d$th cyclotomic polynomial (an $mn$th root of unity which is not an $m$th root of unity is an $n$th root of unity). If $m \neq p$, then $x^{mn} - 1$ has distinct roots modulo $p$. However, by (3), $r$ is a double root. Thus $m = p$. Since $\phi_n(r) \equiv 0 \pmod p$, $r^n \equiv 1 \pmod p$. If $r \equiv 1 \pmod p$, then $q \equiv 1 \pmod p$ and so $(q^n - 1)/(q - 1) \equiv n \pmod p$, a contradiction as $n \neq p$. Thus $p \nmid r^p - 1$, and so $r^{np} \equiv 1 \pmod{p^a}$ by (3). Hence $r^n \equiv 1 \pmod{p^{a-1}}$ by Remark 1, and so $p^a \equiv p \pmod{p^{a-1}}$. This implies $a \leq 2$. Hence $\phi_{np}(r) = 1$, $p$, or $p^2$. If $\phi_{np}(r) = p^2$, then $\phi_n(r) = 1$, which is obviously impossible. If $\phi_{np}(r) = 1$, then

$$(r^{np} - 1)(r - 1) = (r^p - 1)(r^n - 1)$$

by (3). This yields $r \equiv 0 \pmod{r^2}$, a contradiction. If $\phi_{np}(r) = p$, then $\phi_{np}(r) = \phi_n(r)$. Hence $(r^{np} - 1)(r - 1)^2 = (r^p - 1)(r^n - 1)^2$. This is easily seen to be impossible by considering the $r$-adic expansion of both sides.

Next note that if $q = r^{n^e}$, then $r^{n^{e+1}} \equiv 1 \pmod p$. However, if $q \equiv 1 \pmod p$, then $p^a = (q^n - 1)/(q - 1) \equiv n \pmod p$. Thus $r$ has order $n^{e+1}$ modulo $p$, and so $p \equiv 1 \pmod{n^{e+1}}$. This proves (ii).

Finally, note that (iv) follows from (i) and (ii).

THEOREM 1. *In any solution of* (1), $(a, n) = 1$.

*Proof.* Suppose $a = nm$ and set $f = p^h$. Then

$$f^n = (q^n - 1)/(q - 1) \equiv 1 \pmod q.$$

Note that $f \not\equiv 1 \pmod q$ since otherwise $f^n > q^n > (q^n - 1)/(q - 1)$. As $n$ is prime by Lemma 1, we conclude $f$ has order $n \pmod q$, $q = r^b$. Thus

$n|r^{b-1}(r-1)$. If $r \equiv 1 \pmod{n}$ then

$$(q^n - 1)/(q-1) \equiv 0 \pmod{n},$$

a contradiction as $f \equiv 1 \pmod{n}$ by Lemma 1. Hence $r = n$. Now $f^n \equiv 1 \pmod{n^b} \Rightarrow f \equiv 1 \pmod{n^{b-1}}$ by Remark 1. Thus $f - 1 = q(t/n)$ for some integer $t$, and so

$$\left(q\frac{t}{n} + 1\right)^n = \frac{q^n - 1}{q-1} \Rightarrow (q-1)\left(q\frac{t}{n}\right)^n < q^n \Rightarrow q - 1 < \left(\frac{n}{t}\right)^n.$$

By Lemma 1, $q = n^{n^\lambda}$. If $\lambda = 0$, then $q = n$ and $f \equiv f^n \equiv 1 \pmod{n}$, $f > q$, a contradiction as before. Thus $\lambda \geq 1$, and $q \geq n^n$. Now $n^n \leq q < (n/t)^n + 1 > \lambda = t = 1$, so $f - 1 = n^{n-1}$. Since $n$ is odd (as $n$ is a prime and $n \geq 3$), this implies $f$ is even and so $p = 2$. This contradicts Lemma 1 again, and completes the proof of Theorem 1.

Before proving Nagel's result we need a lemma. Let $C(n, k)$ denote the binomial coefficient.

LEMMA 2. *Let $3 \neq p$ be a prime dividing $a$. Then $v_p(C(n,k)a^k) > v_p(C(n,2)a^2)$ for any $2 < k \leq n$.*

*Proof.* If not, then

$$0 \geq v_p\left(\frac{C(n,k)}{C(n,2)}a^{k-2}\right) = v_p\left(\frac{2C(n-2,k-2)a^{k-2}}{k(k-1)}\right).$$

In particular, $(k-2)v_p(a) \leq v_p(k(k-1)) \leq \log_p k$. Then $2^{k-2} \leq p^{k-2} \leq k$, whence $k \leq 4$. For $k = 3$ or 4, the result follows by inspection.

THEOREM 2. (*Nagel*) *If $x, y$ are integers with $|x|, |y| > 1$, then $y^n = x^2 + x + 1$ has no solutions for $n$ not a power of 3.*

*Proof.* We may assume $n \neq 3$ is prime. First note $(y, 3) = 1$ since $9 \nmid (x^2 + x + 1)$. Let $R = Z[\omega]$, $\omega = e^{2\pi i/3}$. So in $R$, $y^n = (x - \omega) \cdot (x - \omega^2)$. Also $(x - \omega, x - \omega^2)|(1 - \omega, y) = 1$. Since $R$ is a principal ideal domain, it follows that

$$x - \omega = \varepsilon(a + b\omega)^n \tag{4}$$

for some unit $\varepsilon$ in $R$ and integers $a$ and $b$. Since the units of $R$ are the sixth root of unity and $(3, n) = 1$, we can assume $\varepsilon = \pm 1$. Reading (4) modulo $b$ yields $b|\omega$ and so $b = \pm 1$.

If $n = 2$, then $x - \omega = \varepsilon(a^2 + 2ab\omega + \omega^2)$, and so $2ab = 1 + \varepsilon$. Thus $|ab| \leq 1$; but this fails for then either $a + b\omega$ is a unit or has norm 3.

Thus $n$ is an odd prime, and so we can take $\varepsilon = 1$. Now (4) also yields $x - \omega \equiv a + b\omega^n \bmod n$. Hence $b = 1$ or $-1$ depending upon whether $n \equiv 2 \bmod 3$ or $n \equiv 1 \bmod 3$. Moreover, if $n \equiv 2 \bmod 3$, $a \equiv x \bmod n$.

First consider the case $n \equiv 2 \bmod 3$. We obtain

$$x = (a + \omega)^n + \omega \equiv na\omega + \omega^2 + \omega \equiv -1 + na\omega \bmod a^2.$$

Hence $na \equiv 0 \bmod a^2$, and so $a = \pm n$, and $x \equiv 1 \bmod a^2$. This is a contradiction as $0 \equiv a \equiv x = -1 \bmod n$.

Now assume $n \equiv 1 \bmod 3$. By replacing $x$ by $-x - 1$ if necessary, we also can assume $x \not\equiv 0 \bmod 3$. It follows from (4) that $a \not\equiv 0 \bmod 3$. We now have

$$x = (a + \omega)^n + \omega = \sum_{k=0}^{n} C(n, k)a^k\omega^{n-k} + \omega.$$

Since the right side is an integer, the coefficient of $\omega$ and $\omega^2$ must be the same. This yields

$$\alpha = \sum_{k \in I} C(n, k)a^k = \sum_{k \in J} C(n, k)a^k = \beta,$$

where $I = \{k \equiv 0 \bmod 3 | 1 \leq k < m\}$ and $J = \{k \equiv 2 \bmod 3 | 1 < k < n\}$. If $p$ is any prime dividing $a$ (note $p \neq 3$), then by Lemma 2, $v_p(\alpha) > v_p(\beta)$. Hence $a = \pm 1$, a contradiction as before.

COROLLARY 1. *Equation* (1) *has no solutions for* $n = 3$ *and* $a \neq 1$.

*Proof*. This follows from Theorems 1 and 2.

In fact Ljunggren [**6**] found all solutions to $y^3 = x^2 + x + 1$. As a consequence, the only nontrivial solutions to $y^n = x^2 + x + 1$ are $n = 3$, $y = 7$, and $x = 18$ or $-19$.

As an application of Theorem 2 we show there are primes $p$ for which a solution of (1) is impossible other than the Fermat primes (as noted in Lemma 1). If $p - 1 = 2^\alpha 3^\beta$, then (1) has a solution $\Leftrightarrow p = (q^3 - 1)/(q - 1)$ by Lemma 1 and Theorem 2. Thus if $p$ is not of the form $q^2 + q + 1$ for $q$ a prime power, then no solution of (1) exists. We conclude that there is no solution of (1) when $p = 19$, 37, 109, 163, or 1459.

In fact Theorem 2 makes solutions of (1) effectively computable for given $p$ when $n = 3$; one need only check whether $p$ is of the form $q^2 + q + 1$ for $q < p$ a prime power. We remark that $7^3 = (18^3 - 1)/(18 - 1)$ shows that both Theorems 1 and 2 are false when $q$ is not restrained to be a prime power.

The techniques used in the proof of Theorem 2 fail to extend to the general case for several reasons. The most crucial of these is the fact that the unit group of the ring of algebraic integers in a cyclotomic field is usually infinite. However, there is a related problem in quadratic extensions of $Q$. Suppose $\alpha$ is an algebraic integer of degree 2. When can $\alpha$ and $\alpha^n$ generate the same order? Clearly this occurs if and only if $\alpha$ and $\alpha^n$ have the same discriminant $\Delta$. Thus we consider the sequence

$$a_k = \frac{\alpha^k - \bar{\alpha}^k}{\sqrt{\Delta}} \tag{5}$$

where $\bar{\alpha}$ is the conjugate of $\alpha$. Hence $Z[\alpha] = Z[\alpha^n]$ if and only if $a_n = \pm 1$. Note $\{a_k\}$ is a defined by

$$a_0 = 0, \quad a_1 = 1, \quad a_{k+2} = Ta_{k+1} - Na_k \tag{6}$$

where $T = \alpha + \bar{\alpha}$ is the trace of $\alpha$ and $N = \alpha\bar{\alpha}$ is the norm of $\alpha$.

THEOREM 3. *Let $\alpha$ be real. Then $Z[\alpha] = Z[\alpha^n]$ for $n > 1$ if and only if $n = 2$ and $T = \pm 1$.*

*Proof.* By replacing $\alpha$ by $\pm\alpha$ or $\pm\bar{\alpha}$ if necessary, we can assume $\alpha \geq |\bar{\alpha}|$. If $\alpha = |\bar{\alpha}|$, then $a_k = 0$ for $k$ even and $a_k > a_1 = 1$ for $1 \neq k$ odd. So $\alpha > |\bar{\alpha}|$. Now (5) yields

$$\sqrt{\Delta}(a_{k+1} - a_k) = \alpha^k(\alpha - 1) - \bar{\alpha}^k(\bar{\alpha} - 1).$$

Since $\alpha^k > |\bar{\alpha}^k|$ and $\alpha - 1 \geq |\bar{\alpha} - 1|$ if $T \neq 1$, it follows that $a_{k+1} > a_k \geq 1$ for $k > 1$. If $T = 1$, $\alpha - 1 = -\bar{\alpha}$, and so

$$\sqrt{\Delta}(a_{k+1} - a_k) = -N(\alpha^{k-1} - \bar{\alpha}^{k-1}) > 0$$

unless $k = 1$. Hence for $k > 2$, $a_k > a_2 \geq 1$.

In the imaginary case there are solutions for $n = 2, 3$ and 5. One can ask whether there are finitely many solutions $(\alpha, n)$. We can give a complete solution for $n = 5$.

THEOREM 4. *$Z[\alpha] = Z[\alpha^5]$ if and only if $\pm\alpha$ or $\pm\bar{\alpha}$ is one of the following*:

(a) $6 + \sqrt{-19}$

(b) $6 + \sqrt{-331}$

(c) $(1 + \sqrt{d})/2$, $d = 3, -7,$ *or* $-11$.

(d) $\sqrt{-1}$.

*Proof.* Consider $a_5$ as defined in (5). Then $a_5 = T^4 - 3NT^2 + N^2$, where $T$ and $N$ are the trace and norm of $\alpha$. Solving the equation $a_5 = \pm 1$

yields

$$N = \frac{3T^2 \pm \sqrt{5T^4}}{2}. \tag{7}$$

Thus $5T^4 \pm 4 = U^2$. Hence

$$\frac{U^2 - 5T^4}{4} = \frac{U - \sqrt{5}\,T^2}{2}\,\frac{U + \sqrt{5}\,T^2}{2} = \pm 1.$$

It follows that $(U + \sqrt{5}\,T^2)/2 = \pm((1 \pm \sqrt{5})/2)^k$ for some $k$, and so $T^2$ is a Fibonacci number. However, the only Fibonacci numbers which are squares are 0, 1 and 144 [**2**]. So $T = 0, \pm 1$ or $\pm 12$. The result now follows from (7).

Note that $Z[\alpha] = Z[\alpha^{10}]$ only holds for $\alpha$ as in (c). Theorem 4 yields a result on solutions of $y^5 = f(x)$.

COROLLARY 2. *Let $f(x)$ be a monic irreducible integral polynomial of degree 2 with roots $\alpha$ and $\bar{\alpha}$. Assume*

(a) *$Z[\alpha]$ is the maximal order of $Q(\alpha)$,*

(b) *5 does not divide the class number of $Z[\alpha]$, and*

(c) *$\alpha$ is not real.*

*Then $y^5 = f(x)$ has no integral solutions for $y \neq 1, 2$, or 3.*

*Proof.* Suppose $y^5 = f(x)$ for integers $x$ and $y$. Hence

$$y^5 = (x - \alpha)(x - \bar{\alpha}).$$

If $P$ is a prime of $Z[\alpha]$ containing both $(x - \alpha)$ and $(x - \bar{\alpha})$, then $P$ contains $\alpha - \bar{\alpha}$ and so is ramified. Thus $P^2 = (m)$, for $m \in Z$. So $y^5 \in P$ implies $x - \alpha$ is divisible by $m$, a contradiction. It follows that $x - \alpha$ and $x - \bar{\alpha}$ are relatively prime. By (b), it now follows that $x - \alpha = u\beta^5$ for some unit $u$. Since $Q(\alpha)$ is an imaginary quadratic extension, $u$ is a fifth power, and so $x - \alpha = \beta^5$. Thus $Z[\alpha] = Z[\beta] = Z[\beta^5]$. Thus by Theorem 4 and (a), $y = \beta\bar{\beta} = 1$, 2 or 3 (corresponding to the solutions in Theorem 4c and 4d).

Although the existence of units of infinite order leads to many difficulties in trying to prove nonexistence of solution to (1′), there are only finitely many solutions for a fixed $p$ and indeed these solutions can be found effectively (but not practically). This follows from the main result in [**10**]. Shorey and Tijdeman [**11**] have used the results in [**10**] to obtain more general results of the same nature. We sketch a proof of the finiteness result in our situation since it is a bit more transparent than [**10**].

THEOREM 5. (*See* [**10**], [**11**].) *For a given prime $p$, there are only finitely many $a, q, n \geq 3$ such that*

$$p^a = \frac{q^n - 1}{q - 1}.$$

*Proof.* By Lemma 1, $p \equiv 1, \bmod n$. So we can take $n$ fixed. Clearly it suffices to bound $a$. Let $\omega$ be a primitive $n$th root of 1. Let $L$ be a finite extension of $Q(\omega)$ such that every ideal in $Q[\omega]$ becomes principal in $L$. Since

$$(p)^a = (q - \omega) \cdots (q - \omega^{n-1})$$

and the factors on the right are relatively prime (as $(q - \omega^i, q - \omega^j) \mid (n, p^a)$), we must have $(p) = (\alpha_1) \cdots (\alpha_{n-1})$, where $(\alpha_t)^a = (q - \omega^i)$. Choose a basis $\beta_1, \ldots, \beta_t$ for the torsion free part of the group of units of $O_L$ such that $|\beta_i| \geq 1$. We can assume $q - \omega = \eta_1 \alpha_1^a$, where

$$\eta_1 = \beta_0^{e_{10}} \beta_1^{e_{11}} \cdots \beta_s^{e_{1s}},$$

$\beta_0$ generates the roots of 1 in $L$ and $0 \leq e_{1t} < a$. Moreover, we shall assume that $q - \omega^j = \eta_j \alpha_j^a$, where $\alpha_j$ and $\alpha_1$ are conjugate. Hence

$$\eta_j = \beta_0^{e_{j0}} \cdots \beta_s^{e_{js}}$$

where $|e_{ji}| < ka$ for some constant $k$. Now $|\alpha_i^a| = |q - \omega^i| / |\eta_i| \leq (p^{a/n-1}) / |\beta_1 \cdots \beta_s|^{ka}$. Hence $|\alpha_i| \leq l$, where $l$ depends only on $p$. Thus by Baker [**1**, Theorem 3.1], if $\Lambda = \log(\eta_1 \alpha_1^a / \eta_j \alpha_j^a)$ for $j > 1$, then $|\Lambda| > ca^{-d}$ for positive constants $c, d$ depending only on $p$. Thus,

$$ca^{-d} < |\Lambda| = \left| \log\left(1 + \frac{\omega^j - \omega}{q - \omega^j}\right) \right| < \frac{4}{|q - \omega^j|} \leq 4p^{n/a}.$$

This bounds $a$ and proves the result.

COROLLARY 3. *If $p$ is an odd prime, there are only finitely many simple groups which have a $p$-complement (i.e., a subgroup of order prime to $p$ and of index a power of $p$).*

*Proof.* This follows from the list of simple groups with subgroups of prime power index in [**4**] and the theorem.

Corollary 3 will hold for $p = 2$ if and only if there are finitely many Mersenne primes.

We finish with a related question. Does the set of primes $p$ for which (1) has a solution have density zero; for this it is sufficient to take $a \geq 2$, and there is only one known solution ($p = 11$).

## REFERENCES

[1] A. Baker, *Transendental Number Theory*, Cambridge Univ. Press, Cambridge, 1975.
[2] J. H. E. Cohn, *On square Fibonacci numbers*, J. London Math. Soc., **39** (1964), 537–540.
[3] W. Feit, *Some consequences of the classification of finite simple groups*, Proceedings of Symposia in Pure Math., Vol. 37 1980, Amer. Math. Soc., Providence, R.I.
[4] R. Guralnick, *Subgroups of prime power index in a simple group*, J. Algebra, **81** (1983), 304–311.
[5] _____, *Subgroups inducing the same permutation representation*, J. Algebra, **81** (1983), 312–319.
[6] W. Ljunggren, *Einige Bemerkungen Uber Die Darstellung Ganzer Zahlen Durch Binare Kubische Farmen Mit Positiver Diskrimante*, Acta Math., **75** (1943), 1–21.
[7] _____, *Some theorems on indeterminate equations of the form* $(x^n - 1)/(x - 1) = y^q$, Norsk. Mat. Tidsskr., **25** (1943), 17–20.
[8] T. Nagel, *Des equations indeterminees* $x^2 + x + 1 = y^n$ *et* $x^2 + x + 1 = 3y^n$, Norsk Matematisk Forening, Skr. (1) no. 2 (1921).
[9] R. Perlis, *On the class numbers of arithmetically equivalent fields*, J. Number Theory, **10** (1978), 489–509.
[10] A. Schinzel and R. Tijdeman, *On the equation* $y^m = P(x)$, Acta Arith., **30** (1976), 199–204.
[11] T. Shorey and R. Tijdeman, *New applications of diophantine approximations to diophantine equations*, Math. Scand., **39** (1976), 5–18.

Received June 15, 1984. The second and third authors were supported in part by NSF Grant MCS 83-01424.

UNIVERSITY OF SOUTHERN CALIFORNIA
LOS ANGELES, CA 90089 - 1113

AND

UNIVERSITY OF CALIFORNIA
LOS ANGELES, CA 90024