

Pacific Journal of Mathematics

ON THE SOLVABILITY OF $x^e \equiv e \pmod{p}$

J. B. MUSKAT

ON THE SOLVABILITY OF $x^e \equiv e \pmod{p}$

J. B. MUSKAT

1. Let e be an integer greater than 1. Let p be a prime $\equiv 1 \pmod{e}$. What conditions must p satisfy if e is an e th power residue, modulo p ?

Let g be a fixed primitive root, modulo p . If $p \nmid a$, define $\text{ind } a$ as the least nonnegative integer t such that $g^t \equiv a \pmod{p}$. For fixed $h, k, 0 \leq h, k \leq e - 1$, define the cyclotomic number (h, k) as the number of solutions of

$$\text{ind } n \equiv h \pmod{e}, \text{ind } (n + 1) \equiv k \pmod{e}, 1 \leq n \leq p - 2.$$

Let $f = (p - 1)/e$. It is well known that

- (1) $(h, k) = (e - h, k - h),$
- (2) $(h, k) = (k, h), \quad f \text{ even},$
 $(h, k) = (k + e/2, h + e/2), \quad f \text{ odd},$
- (3) $\sum_{h=0}^{e-1} (h, k) = \begin{cases} f - 1, & k = 0, \\ f, & 1 \leq k \leq e - 1, \end{cases}$
- (4) $\sum_{k=0}^{e-1} (h, k) = \begin{cases} f - 1, & f \text{ even}, h = 0, \\ f - 1, & f \text{ odd}, h = e/2, \\ f, & \text{otherwise.} \end{cases}$

Let ζ_e denote a primitive e th root of unity. Define the primitive e th power character $\chi_p(a) = \zeta_e^{\text{ind } a}$ for $a \not\equiv 0 \pmod{p}$.

THEOREM 1. $\text{ind } e \equiv (p - 1)/2 - \sum_{h=1}^{e-1} (h, 0)h \pmod{e}.$

Proof. Let $z \equiv g^f \pmod{p}$. Then

$$e \equiv \prod_{k=1}^{e-1} (1 - z^k) \pmod{p}.$$

For a fixed $v, 0 \leq v \leq e - 1$, let \sum_v and \prod_v denote the sum and the product, respectively, over all $n, 1 \leq n \leq p - 1$, such that $\text{ind } n \equiv v \pmod{e}$. Define

$$\sum'_v = \sum_v, v \neq 0; \sum'_0 = \sum_{\substack{0 \\ n \neq 1}}.$$

Then

Received April 17, 1963. This research was supported in part by the National Science Foundation, Research Grant No. G 11309. Reproduction in whole or in part is permitted for any purpose of the United States Government.

$$x^f - z^v \equiv \prod_v (x - n) \pmod{p} .$$

Set $x = 1$. Then

$$1 - z^v \equiv \prod_v (1 - n) \pmod{p} .$$

Thus

$$\begin{aligned} \text{ind } e &\equiv \sum_{v=1}^{e-1} \sum_v \text{ind } (1 - n) \\ &\equiv \sum_{v=0}^{e-1} \sum'_v \text{ind } (1 - n) - \sum'_0 \text{ind } (1 - n) \\ &\equiv \sum_{u=1}^{p-1} \text{ind } u - \text{ind } 1 - \sum'_0 [\text{ind } (-1) + \text{ind } (n - 1)] \\ &\equiv fe(e - 1)/2 - (f - 1)ef/2 - \sum'_0 \text{ind } (n - 1) \\ &\equiv ef/2 - \sum_{h=1}^{e-1} (h, 0)h \pmod{e} . \end{aligned}$$

COROLLARY 1. *If e is odd, $\text{ind } e \equiv \sum_{h=1}^{(e-1)/2} h[(e - h, 0) - (h, 0)] \pmod{e}$.*

2. Hereafter, let e be an odd prime.

Define the Jacobi sum

$$\pi(j, k) = \sum_{n=2}^{p-1} \chi_p^j(n) \chi_p^k(1 - n) = \sum_{n=1}^{p-2} \chi_p^k(n) \chi_p^j(n + 1), \quad j, k, j + k \not\equiv 0 \pmod{e} .$$

It can be shown easily that

$$\pi(vk, k) = \sum_{i=0}^{e-1} B(i, v) \zeta_e^{ki} ,$$

where

$$B(i, v) = \sum_{h=0}^{e-1} (h, i - vh) .$$

Also, if v' is any solution of $vv' \equiv 1 \pmod{e}$,

$$(5) \quad B(i, v) = B(i, e - v - 1) = B(iv', v') \quad [3, \text{p. } 97] .$$

It will be demonstrated that for e an odd prime, $\text{ind } e \pmod{e}$ can be expressed as a linear combination of $B(i, v)$, the rational integral coefficients of Jacobi sums. N. C. Ankeny gave a similar criterion, expressed in terms of the coefficients of the e th power Gaussian sum

$$\tau(\chi_p)^e = p \prod_{k=1}^{e-2} \pi(1, k) ,$$

and a variation of this criterion was found by the author [2, pp. 103, 108].

Set

$$S = \sum_{i=1}^{(e-1)/2} i \sum_{v=1}^{e-2} [B(e-i, v) - B(i, v)].$$

THEOREM 2. *If e is an odd prime, then $e \text{ ind } e \equiv S \pmod{e^2}$.*

Proof. If

$$\begin{aligned} 1 \leq i \leq e-1, \sum_{v=1}^{e-2} B(i, v) &= \sum_{v=1}^{e-2} \sum_{h=0}^{e-1} (h, i-vh) \\ &= \sum_{v=1}^{e-2} (0, i) + \sum_{h=1}^{e-1} \sum_{v=1}^{e-2} (h, i-vh) \\ &= (e-2)(0, i) + \sum_{h=1}^{e-1} \left[-(h, i) - (h, i+h) + \sum_{v=0}^{e-1} (h, i-vh) \right] \\ &= (e-2)(0, i) + \sum_{h=1}^{e-1} [-(h, i) - (e-h, i) + f], \text{ by (1) and (4),} \\ &= (e-2)(0, i) - 2[f - (0, i)] + (e-1)f, \text{ by (3),} \\ &= (i, 0)e + (e-3)f, \text{ by (2).} \end{aligned}$$

Thus,

$$(6) \quad e[(e-i, 0) - (i, 0)] = \sum_{v=1}^{e-2} [B(e-i, v) - B(i, v)].$$

Substituting (6) into Corollary 1 yields the theorem.

COROLLARY 2. *If e is an odd prime, e is an e th power residue, modulo p , if and only if $S \equiv 0 \pmod{e^2}$.*

C. E. Bickmore presented without proof criteria (attributed to L. Tanner) for $e = 5$ and $e = 7$ [1, pp. 29, 36]. These criteria, (7) and (8), follow from Theorem 2:

Hereafter, let $B(i, 1) = d_i$, $B(i, 2) = c_i$.

If $e = 5$, $B(i, 3) = B(i, 1)$, $B(i, 2) = B(3i, 3) = B(3i, 1)$, by (5).

$$\begin{aligned} 5 \text{ ind } 5 &\equiv [2(d_4 - d_1) + (d_2 - d_3)] + 2[2(d_3 - d_2) + (d_4 - d_1)] \\ &\equiv 4(d_4 - d_1) + 3(d_3 - d_2) \pmod{25}. \end{aligned}$$

Multiply the congruence by 6:

$$(7) \quad 5 \text{ ind } 5 \equiv d_1 - d_4 + 7(d_2 - d_3) \pmod{25}.$$

(Theorem 1 is a generalization of a proof of (7) which Emma Lehmer communicated to the author.)

If $e = 7$, $B(i, 5) = B(i, 1)$, $B(i, 3) = B(5i, 5) = B(5i, 1)$, $B(i, 4) = B(i, 2)$, by (5). Also, $B(1, 2) = B(2, 2) = B(4, 2)$, $B(3, 2) = B(5, 2) = B(6, 2)$, by

(1) and (2).

$$\begin{aligned}
 7 \text{ ind } 7 &\equiv [2(d_6 - d_1) + 2(c_6 - c_1) + (d_2 - d_5)] \\
 &\quad + 2[2(d_5 - d_2) + 2(c_5 - c_2) + (d_4 - d_3)] \\
 &\quad + 3[2(d_4 - d_3) + 2(c_4 - c_3) + (d_6 - d_1)] \\
 &\equiv 5(d_6 - d_1) + 3(d_5 - d_2) + 8(d_4 - d_3) \pmod{49}.
 \end{aligned}$$

Multiply the congruence by 39:

$$(8) \quad 28 \text{ ind } 7 \equiv d_1 - d_6 - 19(d_2 - d_5) - 18(d_3 - d_4) \pmod{49}.$$

The author is grateful to the referee for his helpful suggestions.

BIBLIOGRAPHY

1. C. E. Bickmore, *On the Numerical Factors of $a^n - 1$* (Second Notice), *The Messenger of Mathematics*, **26** (1896), 1-38.
2. J. B. Muskat, *On Certain Prime Power Congruences*, *Abhandlungen aus dem mathematischen Seminar der Universität Hamburg*, **26** (1963), 102-110.
3. A. L. Whiteman, *The Cyclotomic Numbers of Order Ten*, *Proceedings of the Symposia in Applied Mathematics*, Vol. 10, 95-111, American Mathematical Society, Providence, Rhode Island, 1960.

UNIVERSITY OF PITTSBURGH

PACIFIC JOURNAL OF MATHEMATICS

EDITORS

ROBERT OSSERMAN
Stanford University
Stanford, California

M. G. ARSOVE
University of Washington
Seattle 5, Washington

J. DUGUNDJI
University of Southern California
Los Angeles 7, California

LOWELL J. PAIGE
University of California
Los Angeles 24, California

ASSOCIATE EDITORS

E. F. BECKENBACH

B. H. NEUMANN

F. WOLF

K. YOSIDA

SUPPORTING INSTITUTIONS

UNIVERSITY OF BRITISH COLUMBIA
CALIFORNIA INSTITUTE OF TECHNOLOGY
UNIVERSITY OF CALIFORNIA
MONTANA STATE UNIVERSITY
UNIVERSITY OF NEVADA
NEW MEXICO STATE UNIVERSITY
OREGON STATE UNIVERSITY
UNIVERSITY OF OREGON
OSAKA UNIVERSITY
UNIVERSITY OF SOUTHERN CALIFORNIA

STANFORD UNIVERSITY
UNIVERSITY OF TOKYO
UNIVERSITY OF UTAH
WASHINGTON STATE UNIVERSITY
UNIVERSITY OF WASHINGTON
* * *
AMERICAN MATHEMATICAL SOCIETY
CALIFORNIA RESEARCH CORPORATION
SPACE TECHNOLOGY LABORATORIES
NAVAL ORDNANCE TEST STATION

Pacific Journal of Mathematics

Vol. 14, No. 1

May, 1964

Richard Arens, <i>Normal form for a Pfaffian</i>	1
Charles Vernon Coffman, <i>Non-linear differential equations on cones in Banach spaces</i>	9
Ralph DeMarr, <i>Order convergence in linear topological spaces</i>	17
Peter Larkin Duren, <i>On the spectrum of a Toeplitz operator</i>	21
Robert E. Edwards, <i>Endomorphisms of function-spaces which leave stable all translation-invariant manifolds</i>	31
Erik Maurice Ellentuck, <i>Infinite products of isols</i>	49
William James Firey, <i>Some applications of means of convex bodies</i>	53
Haim Gaifman, <i>Concerning measures on Boolean algebras</i>	61
Richard Carl Gilbert, <i>Extremal spectral functions of a symmetric operator</i>	75
Ronald Lewis Graham, <i>On finite sums of reciprocals of distinct nth powers</i>	85
Hwa Suk Hahn, <i>On the relative growth of differences of partition functions</i>	93
Isidore Isaac Hirschman, Jr., <i>Extreme eigen values of Toeplitz forms associated with Jacobi polynomials</i>	107
Chen-jung Hsu, <i>Remarks on certain almost product spaces</i>	163
George Seth Innis, Jr., <i>Some reproducing kernels for the unit disk</i>	177
Ronald Jacobowitz, <i>Multiplicativity of the local Hilbert symbol</i>	187
Paul Joseph Kelly, <i>On some mappings related to graphs</i>	191
William A. Kirk, <i>On curvature of a metric space at a point</i>	195
G. J. Kurowski, <i>On the convergence of semi-discrete analytic functions</i>	199
Richard George Laatsch, <i>Extensions of subadditive functions</i>	209
V. Marić, <i>On some properties of solutions of $\Delta\psi + A(r^2)X\nabla\psi + C(r^2)\psi = 0$</i> ...	217
William H. Mills, <i>Polynomials with minimal value sets</i>	225
George James Minty, Jr., <i>On the monotonicity of the gradient of a convex function</i>	243
George James Minty, Jr., <i>On the solvability of nonlinear functional equations of 'monotonic' type</i>	249
J. B. Muskat, <i>On the solvability of $x^e \equiv e \pmod{p}$</i>	257
Zeev Nehari, <i>On an inequality of P. R. Bessack</i>	261
Raymond Moos Redheffer and Ernst Gabor Straus, <i>Degenerate elliptic equations</i>	265
Abraham Robinson, <i>On generalized limits and linear functionals</i>	269
Bernard W. Roos, <i>On a class of singular second order differential equations with a non linear parameter</i>	285
Tôru Saitô, <i>Ordered completely regular semigroups</i>	295
Edward Silverman, <i>A problem of least area</i>	309
Robert C. Sine, <i>Spectral decomposition of a class of operators</i>	333
Jonathan Dean Swift, <i>Chains and graphs of Ostrom planes</i>	353
John Griggs Thompson, <i>2-signalizers of finite groups</i>	363
Harold Widom, <i>On the spectrum of a Toeplitz operator</i>	365