Pacific Journal of Mathematics

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

J. B. MUSKAT

Vol. 14, No. 1 May 1964

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 eth power residue, modulo p?

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

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

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

$$(1) \qquad (h, k) = (e-h, k-h) ,$$

$$(2) \qquad \begin{aligned} (h, k) &= (k, h) , && f \text{ even} , \\ (h, k) &= (k + e/2, h + e/2) , && f \text{ odd} , \end{aligned}$$

$$(3) \qquad \sum_{h=0}^{e-1} (h, k) = \begin{cases} f-1 , & k = 0 , \\ f , & 1 \leqq k \leqq e-1 , \end{cases}$$

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

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

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

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

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

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

$$\begin{aligned} \operatorname{ind} e &\equiv \sum_{v=1}^{e-1} \sum_v \operatorname{ind} (1 - n) \\ &\equiv \sum_{v=0}^{e-1} \sum_v' \operatorname{ind} (1 - n) - \sum_0' \operatorname{ind} (1 - n) \\ &\equiv \sum_{u=1}^{p-1} \operatorname{ind} u - \operatorname{ind} 1 - \sum_0' [\operatorname{ind} (-1) + \operatorname{ind} (n - 1)] \\ &\equiv fe(e - 1)/2 - (f - 1)ef/2 - \sum_0' \operatorname{ind} (n - 1) \\ &\equiv ef/2 - \sum_{h=1}^{e-1} (h, 0)h \pmod{e} . \end{aligned}$$

COROLLARY 1. *If e is odd, 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

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

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 $vv' \equiv 1 \pmod{e}$,

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

It will be demonstrated that for e an odd prime, 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 eth 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 ind $e \equiv S \pmod{e^2}$.*

Proof. If

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

Thus,

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

Substituting (6) into Corollary 1 yields the theorem.

COROLLARY 2. *If e is an odd prime, e is an eth 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:

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

(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:

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

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

Printed in Japan by International Academic Printing Co., Ltd., Tokyo, Japan

Pacific Journal of Mathematics
Vol. 14, No. 1 May, 1964