ACTA ARITHMETICA
XLIII (1984)

Criterion for 2 to be an lth power

by

J. C. PARNAMI, M. K. AGRAWAL, SATINDER PALL, and A. R. RAJWADE
(Chandigarh, India)

1. Introduction. Jacobi [3] has given necessary and sufficient conditions for primes $q < 37$ to be cubes modulo primes $p \equiv 1 \pmod 3$. For example he proves the following

PROPOSITION 1. (i) *2 is a cube* $\bmod p$ *if and only if* $L \equiv 0 \pmod 2$, *and*

(ii) *3 is a cube* $\bmod p$ *if and only if* $M \equiv 0 \pmod 3$,

where (L, M) *is one of the exactly two solutions* $(L, \pm M)$ *of the diophantine system (Gauss)*:

$$4p = L^2 + 27M^2, \quad L \equiv 1 \pmod 3 \tag{1}$$

Emma Lehmer [4] proves the following results:

PROPOSITION 2. *Let* $p \equiv 1 \pmod 5$ *be a prime, then*

(i) *2 is a fifth power* $\bmod p$ *if and only if* $x \equiv 0 \pmod 2$,

(ii) *3 is a fifth power* $\bmod p$ *if and only if* $u \equiv v \equiv 0 \pmod 3$,

where (x, u, v, w) *is one of the exactly four solutions* (x, u, v, w), $(x, -u, -v, w)$, $(x, v, -u, -w)$, $(x, -v, u, -w)$ *of the diophantine system* (Dickson):

$$16p = x^2 + 50u^2 + 50v^2 + 125w^2, \quad xw = v^2 - 4uv - u^2, \quad x \equiv 1 \pmod 5. \tag{2}$$

Leonard and Williams [5] prove the following

PROPOSITION 3. *Let* $p \equiv 1 \pmod 7$ *be a prime, then*

(i) *2 is a seventh power* $\bmod p$ *if and only if* $x_1 \equiv 0 \pmod 2$, *and*

(ii) *3 is a seventh power* $\bmod p$ *if and only if* $x_5 \equiv x_6 \equiv 0 \pmod 3$,

where $(x_1, x_2, \ldots, x_6)$ *is one of the exactly six non-trivial solutions*

$$(x_1, x_2, x_3, x_4, x_5, x_6), \quad (x_1, -x_3, x_4, x_2, -\tfrac{1}{2}(x_5 + 3x_6), \tfrac{1}{2}(x_5 - x_6)),$$

$$\left(x_1, -x_4, x_2, -x_3, \tfrac{1}{2}(-x_5+3x_6), -\tfrac{1}{2}(x_5+x_6)\right), \quad (x_1, -x_2, -x_3, -x_4, x_5, x_6),$$
$$\left(x_1, x_3, -x_4, -x_2, \tfrac{1}{2}(-x_5-3x_6), -\tfrac{1}{2}(x_5-x_6)\right),$$
$$\left(x_1, x_4, -x_2, x_3, \tfrac{1}{2}(-x_5+3x_6), -\tfrac{1}{2}(x_5+x_6)\right)$$

(the two trivial ones being $(-6t, \pm 2u, \pm 2u, \mp 2u, 0, 0)$, where $p = t^2+7u^2$, $t \equiv 1 \pmod 7$) of the diophantine system of equations

$$\begin{aligned}
&\text{(i)} && 72p = 2x_1^2+42(x_2^2+x_3^2+x_4^2)+343(x_5^2+3x_6^2),\\
&\text{(ii)} && 12x_2^2-12x_4^2+147x_5^2-441x_6^2+56x_1x_6+24x_2x_3-24x_2x_4+48x_3x_4+\\
& && \qquad +98x_5x_6 = 0,\\
(3)\quad &\text{(iii)} && 12x_3^2-12x_4^2+49x_5^2-147x_6^2+28x_1x_5+28x_1x_6+48x_2x_3+\\
& && \qquad +24x_2x_4+24x_3x_4+490x_5x_6 = 0,\\
&\text{(iv)} && x_1 \equiv 1 \pmod 7.
\end{aligned}$$

Leonard, Mortimer and Williams [6] prove the following

PROPOSITION 4. *Let $p \equiv 1 \pmod{11}$ be a prime, then 2 is an eleventh power* mod$p$ *if and only if a certain condition involving solutions of a very complicated diophantine system holds* (the exact statement may be seen in [6]).

As soon as a diophantine system (such as the ones given above) is available for primes $p \equiv 1 \pmod l$ (l an odd prime), it is not unreasonable to expect that a criterion for some small primes q to be lth powers modulo p may be worked out, the cases $l = 3, 5, 7$, $q = 2, 3$ and $l = 11$, $q = 2$ being stated above. More work has been done on this topic by various authors, for instance the cases $l = 7, q = 2, 3$ have been treated somewhat differently by Alderson [1], the case $q \equiv 1 \pmod l$ has been considered by Ankeny [2], the case $q = l$ by Ankeny [2] and Muskat [7] and the cases $l = 5$, $q \leqslant 19$ by Williams [9].

Parnami, Agrawal and Rajwade [8] have given such a diophantine system for all odd primes l. Our object is to give a criterion for 2 to be an lth power modulo p (p a prime $\equiv 1 \pmod l$) in terms of the variables of the essentially unique solution of the diophantine system of Parnami, Agrawal and Rajwade.

2. The main result.

THEOREM. *Let $p \equiv 1 \pmod l$, then 2 is an l-th power modulo p if and only if*

$$a_1+a_2+\ldots+a_{l-1} \equiv 0 \pmod 2$$

where $(a_1, a_2, \ldots, a_{l-1})$ is one of the exactly $l-1$ solutions of the diophantine system of equations

$$\text{(i)}\quad p = \sum_{i=1}^{l-1} a_i^2 - \sum_{i=1}^{l-1} a_i a_{i+1},$$

$$\text{(ii)}\quad \sum_{i=1}^{l-1} a_i a_{i+1} = \sum_{i=1}^{l-1} a_i a_{i+2} = \ldots = \sum_{i=1}^{l-1} a_i a_{i+l-1},$$

(4) (iii) $p \nmid \prod_{\lambda(2k)>k} \left(\sum_{i=1}^{l-1} a_i \zeta^i\right)^{\sigma_k}$, *where $\zeta = e^{2\pi i}/l$ and where $\lambda(n)$ is the least non-negative residue of n modulo l and σ_k is the automorphism: $\zeta \to \zeta^k$,*

(iv) $1+a_1+\ldots+a_{l-1} \equiv 0 \pmod l$,

(v) $a_1+2a_2+\ldots+(l-1)a_{l-1} \equiv 0 \pmod l$

(in (i) and (ii) the subscripts of the a's are to be considered modulo l and a_0 is taken to be 0).

Note that any of the $l-1$ solutions gives the same condition since these solutions are just permutations of each other.

Remark. The right hand side of (i) of (4) is a positive definite quadratic form since it can be written as

$$\tfrac{1}{2}\left[a_1^2+\left\{\sum_{i=1}^{l-2}(a_i-a_{i+1})^2\right\}+a_{l-1}^2\right] \qquad (\text{note that } a_l = 0).$$

Hence all the solutions of (i) alone can be obtained in a finite number of steps. Of these only those solutions $(a_1, a_2, \ldots, a_{l-1})$ are to be retained which also satisfy (ii)–(v) of (4).

For completeness we give a (new) proof of the following known

LEMMA. *2 is an l-th power modulo p if and only if the cyclotomic constant $(0, 0)_l$ is odd.*

Proof. Let $X_{00} = \{x \in F_p^* \mid x$ and $x+1$ are both lth powers$\}$. Then

(5) 2 is an lth power if and only if $1 \in X_{00}$.

On the other hand $X_{00} = \bigcup_{x \in X_{00}} \{x, 1/x\}$. In this union the two sets $\{x, 1/x\}$ and $\{y, 1/y\}$ are either the same or disjoint. Further $x = 1/x$ if and only if $x = 1$ since x cannot take the value -1. Thus $|X_{00}|$ is even unless $1 \in X_{00}$, i.e. $|X_{00}|$ is odd if and only if $1 \in X_{00}$. This, together with (5), gives the lemma, noting that $(0, 0)_l = |X_{00}|$.

Proof of the theorem.

$$l^2(0, 0) = \sum_{0 \leqslant i,j \leqslant l-1}\sum J(i, j) \qquad (J \text{ being the Jacobi function})$$
$$= q-2-2(l-1)+\sum_{1 \leqslant i,j \leqslant l-1}\sum J(i, j)$$
$$(\text{since } J(0, 0) = q-2,\ J(i, 0) = J(0, i) = -1\ (i \neq 0)).$$

$$= q-2-2(l-1)+\sum_{j=1}^{l-1}\operatorname{Tr}(J(1,j))$$

$$= q-2-2(l-1)+\sum_{j=1}^{(l-3)/2}\operatorname{Tr}[J(1,j)+J(1,l-1-j)]+ \\ +\operatorname{Tr}\left[J\left(1,\frac{l-1}{2}\right)\right]+\operatorname{Tr}[J(1,l-1)]$$

$$= q-2-2(l-1)+2\sum_{j=1}^{(l-3)/2}\operatorname{Tr}[J(1,j)]+\operatorname{Tr}\left[J\left(\frac{l-1}{2},\frac{l-1}{2}\right)\right]+\operatorname{Tr}[J(1,0)]$$

(since the respective replacement in the J's are equal by the Stickelberger relations $J(a,b)=J(b,c)=J(c,a)$ if $a+b+c\equiv 0 \pmod l$) $\equiv 1+\operatorname{Tr}[J(1,1)]$ (modulo 2) since $J(1,1)$ is a conjugate of $J\left(\frac{l-1}{2},\frac{l-1}{2}\right)$ and $\operatorname{Tr}[J(1,0)]=\operatorname{Tr}(-1)=-(l-1)\equiv 0 \pmod 2$.

But now $\operatorname{Tr}[J(1,1)]$ is even if and only if $a_1+a_2+\ldots+a_{l-1}$ is even since $J(1,1)=a_1\zeta+a_2\zeta^2+\ldots+a_{l-1}\zeta^{l-1}$ so that $-\operatorname{Tr}[J(1,1)]=a_1+a_2+\ldots+a_{l-1}$. Thus $(0,0)_l$ is odd if and only if $a_1+a_2+\ldots+a_{l-1}$ is even, i.e. 2 is an lth power if and only if $a_1+a_2+\ldots+a_{l-1}$ is even. This completes the proof.

3. Examples. I. Let $l=11$, $p=67$. A solution $(a_1,a_2,\ldots,a_{10})$ of the system (4) is $(-6,-2,-4,0,-4,-5,-2,2,-2,0)$ and the remaining nine solutions are $(a_i,a_{2i},\ldots,a_{10i})$ $(i=2,3,\ldots,10)$. Here $a_1+a_2+\ldots+a_{10}$ is odd and so 2 is not an 11th power modulo 67.

II. $l=13$, $p=53$. Here a solution $(a_1,a_2,\ldots,a_{12})$ of the system (4) is $(-4,-2,2,0,2,2,-1,2,-2,0,-2,2)$ and the remaining eleven are $(a_i,a_{2i},\ldots,a_{12i})$ $(i=2,3,\ldots,12)$. Here $a_1+a_2+\ldots+a_{12}$ is odd and so 2 is not a 13th power modulo 53.

III. $l=13$, $p=131$. As in example II, a solution $(a_1,a_2,\ldots,a_{12})$ is $(6,2,4,0,6,0,-6,2,1,4,4,2)$ and as $a_1+a_2+\ldots+a_{12}$ is again odd, 2 is not a 13th power modulo 131.

References

[1] H. P. Alderson, *On the septimic character of 2 and 3*, Proc. Camb. Phil. Soc. 74 (1973), pp. 421–433.
[2] N. C. Ankeny, *Criterion for r-th power residuacity*, Pacific J. Math. 10 (1960), pp. 1115–1124.
[3] K. G. J. Jacobi, *De residuis cubicis commentatio numerosa*, Crelle 2 (1827), pp. 66–69.

[4] E. Lehmer, *The quintic character of 2 and 3*, Duke Math. J. 18 (1951), pp. 11–18.
[5] P. A. Leonard and K. S. Williams, *The septic character of 2, 3, 5 and 7*, Pacific J. Math. 52 (1974), pp. 143–147.
[6] P. A. Leonard, B. C. Mortimer and K. S. Williams, *The eleventh power character of 2*, Crelle 286/287 (1976), pp. 213–222.
[7] J. B. Muskat, *On the solvability of $x^e\equiv e \pmod p$*, Pacific J. Math. 14 (1964), pp. 257–260.
[8] J. C. Parnami, M. K. Agrawal and A. R. Rajwade, *Jacobi sums and cyclotomic numbers over a finite field*, Acta Arith. 41 (1982), pp. 1–13.
[9] K. S. Williams, *Explicit criteria for quintic residuacity*, Math. Comp. 30 (1974), pp. 1–6.

DEPARTMENT OF MATHEMATICS
PANJAB UNIVERSITY
Chandigarh, India

Received on 10.5.1982
and in revised form on 10.1.1983 (1305)