PAIRS OF CONSECUTIVE POWER RESIDUES OR NON-RESIDUES

J. H. JORDAN

1. Introduction. For a positive integer k and a prime $p \equiv 1 \pmod{k}$, there is a proper subgroup, R, of the multiplicative group (mod p) consisting of the kth power residues (mod p). A necessary and sufficient condition that an integer t be an element of R is that the congruence $x^k \equiv t \pmod{p}$ be solvable. The cosets, not R, formed with respect to R are called classes of kth power non-residues, and form with R a cyclic group of order k. Let ρ be a primitive kth root of unity and let S be a class of non-residues that is a generator of this cyclic group. There is a kth power character χ (mod p) such that

$$\chi(a) = \rho^j \quad \text{if } a \in S^j, \qquad 0 \leqslant j < k.$$

For a kth power character, χ (mod p), define a function g on the positive integers such that

$$g(a) = j \quad \text{when } \chi(a) = \rho^j.$$

The function g then has the property that

$$g(ab) \equiv g(a) + g(b) \pmod{k}.$$

It is easy to see that the function g and the character χ are isomorphic.

Brauer **(1)** proved that for any positive integer m and for p sufficiently large there exists a positive integer r such that

$$\text{(I)} \qquad g(r) = g(r+1) = \ldots = g(r+m-1) = 0.$$

Lehmer, Lehmer, and Mills **(4)** defined $r(k, m, p)$ to be the least r for which (I) holds and $\Lambda(k, m) = \max\{r(k, m, p)\}$ where the maximum is taken over all primes except for a finite exceptional set where (I) fails to occur.

Let P^* denote an exceptional prime. The following results have been established:

Trivially

(1) $\Lambda(2, 2) = 9$, $P^* = 2, 3, 5$.

Dunton **(2)** showed that

(2) $\Lambda(3, 2) = 77$, $P^* = 2, 7, 13$.

Mills and Bierstedt **(5)** showed that

(3) $\Lambda(4, 2) = 1224$, $P^* = 2, 3, 5, 13, 17, 41$.

Received June 17, 1963.

https://doi.org/10.4153/CJM-1964-030-6 Published online by Cambridge University Press

Lehmer, Lehmer, and Mills **(4)** showed that

(4) $\Lambda(5, 2) = 7888$, $P^* = 2, 11, 41, 71, 101$

and

(5) $\Lambda(6, 2) = 202124$, $P^* = 2, 3, 5, 7, 13, 19, 43, 61, 97, 157, 277$.

The IBM 701 and 704 assisted in the establishment of (4) and (5).

It is the purpose of this paper to ask a little less than (I) and investigate the corresponding results.

For any integer m, replace the condition (I) by

$$\text{(II)} \qquad g(r) = g(r+1) = g(r+2) = \ldots = g(r+m-1).$$

This now allows that the consecutive integers can be either in the class of residues or in one of the classes of non-residues.

Let $a(k, m, p)$ be the least positive integer for which (II) holds and let $\Lambda^*(k, m) = \max\{a(k, m, p)\}$, where the maximum is taken over all primes except for a finite exceptional set where (II) fails to occur. Since $a(k, m, p) \leqslant r(k, m, p)$, it follows that $\Lambda^*(k, m) \leqslant \Lambda(k, m)$.

THEOREM 1:

(1) $\Lambda^*(2, 2) = 3$, $P^* = 2, 3$.

(2) $\Lambda^*(3, 2) = 8$, $P^* = 2$.

(3) $\Lambda^*(4, 2) = 20$, $P^* = 2, 3, 5$.

(4) $\Lambda^*(5, 2) = 44$, $P^* = 2$.

(5) $\Lambda^*(6, 2) = 80$, $P^* = 2, 3, 7$.

(6) $\Lambda^*(7, 2) = 343$, $P^* = 2$.

Lehmer and Lehmer **(3)** proved that

$$\Lambda(2k, 3) = \infty \quad \text{and } \Lambda(k, 4) = \infty \quad \text{for } k < 1048909.$$

R. Graham (unpublished) extended the result to

$$\Lambda(k, w) = \infty \quad \text{for all } k \text{ and } w \geqslant 4.$$

The corresponding results for Λ^* are given in the following theorem.

THEOREM 2:

(1) $\Lambda^*(2k, 3) = \infty$.

(2) $\Lambda^*(k, w) = \infty, \quad w \geqslant 4$.

2. On the proof of Theorem 1.

A very slight generalization that tends to emphasize the flavour of the proof is to consider not just kth power characters but to discuss functions, f, for which

$$\text{(III)} \qquad f(ab) \equiv f(a) + f(b) \pmod{k},$$

where the a and b are positive integers. Clearly $f(1) \equiv 0 \pmod{k}$ for all functions f with this multiplicative property.

Because of the many isomorphisms of a cyclic group many cases can be brushed aside by an argument essentially the one just presented. When this is asserted in the following proofs the comment "... need not be considered" will be made.

Functions f with property (III) need only be defined at the primes to be completely determined.

In each of the parts of the proof all possible functions f (mod k) will be considered and in each case a b and an i will be determined such that

$$f(b) = f(b+1) = i.$$

Since any given kth power residue character is isomorphic to an f, they will also be handled, with the possible exception of the kth power residue characters associated with the primes used in proving the theorem.

An argument table will be constructed for each of four parts of the proof. The table will have the b and the i and the values of f for the small primes that were used to determine the b and the i. When the value of f at a small prime is arbitrary, a dash will be placed in that column.

The value $a(k, m, p) \leqslant b$ for the primes, p, that have their kth power residue character in agreement with the f's at the primes pertinent to that segment of the argument. It then follows that $\Lambda^*(k, 2) \leqslant \max\{b\}$. A function f is exhibited such that the smallest b for which $f(b) = f(b+1) = i$, for some i, is equal to $\max\{b\}$. A theorem proved by Mills **(6)** implies that there are infinitely many primes that have a kth power character that agrees with f on this finite set of primes. Therefore $\Lambda^*(k, 2) = \max\{b\}$, completing the argument.

The proofs of (5) and (6) will be omitted because of their length.

3. The tables.

Proof of (1):

$f(2)$	$f(3)$	b	i
0	–	1	0
1	1	2	1
1	0	3	0

$\Lambda^*(2, 2) \leqslant 3$ except for $p = 2$ or 3.
$f(2) = 1$ and $f(3) = 0$ implies $\Lambda^*(2, 2) = 3$.

Proof of (2):

$f(2)$	$f(3)$	b	i
0	–	1	0
1	1	2	1
1	2	3	2
1	0	8	0

https://doi.org/10.4153/CJM-1964-030-6 Published online by Cambridge University Press

$f(2) = 2$ need not be considered.
$\Lambda^*(3, 2) \leqslant 8$ except for $p = 2$.
$f(2) = 1, f(3) = f(5) = 0$, and $f(7) = 2$ imply $\Lambda^*(3, 2) = 8$.

Proof of (3):

f: 2, 3, 5, 7	b	i
0, –, –, –	1	0
1, 1, –, –	2	1
1, 2, –, –	3	2
1, 0, 0, –	15	0
1, 0, 1, –	5	1
1, –, 2, –	4	2
1, 0, 3, –	9	0
1, 3, 0, –	5	0
1, 3, 1, –	9	2
1, 3, –, 0	6	0
1, 3, 3, 1	14	2
1, –, –, 3	7	3
1, 3, 3, 2	20	1
2, 2, –, –	2	2
2, 0, –, –	3	0
2, 3, –, –	8	2
2, 1, –, –	8	2

$f(2) = 3$ need not be considered.
$\Lambda^*(4, 2) \leqslant 20$ except for $p = 2, 3$, or 5.
$f(2) = 1, f(3) = f(5) = 3$, and $f(p) = 2$ for $p = 7, 11, 13, 17, 19$ implies $\Lambda^*(4, 2) = 20$.

Proof of (4): $k = 5$

f: 2, 3, 5, 7, 11	b	i
0, –, –, –, –	1	0
1, 1, –, –, –	2	1
1, 2, –, –, –	3	2
1, 4, –, –, –	8	3
1, 0, 1, –, –	5	1
1, –, 2, –, –	4	2
1, 0, 4, –, –	24	3
1, 0, –, 1, –	6	1
1, –, –, 3, –	7	3
1, 0, 0, 2, –	35	2
1, 0, 0, 4, –	14	0
1, –, 0, –, 1	10	1
1, 0, –, –, 2	11	2
1, 0, 0, –, 3	44	0
1, 0, –, 0, 4	21	0
1, 0, –, –, 0	32	0

https://doi.org/10.4153/CJM-1964-030-6 Published online by Cambridge University Press

f: 2, 3, 5, 7, 11	b	i
1, 0, 3, 2, –	14	3
1, 0, 3, 4, –	35	2
1, 0, 3, 0, –	20	0
1, 3, 4, –, –	5	4
1, 3, 0, –, –	9	1
1, 3, 1, –, –	15	4
1, 3, 3, –, –	24	1

$f(2) = i$, $i = 2, 3, 4$, need not be considered. $\Lambda^*(5, 2) \leqslant 44$ with the exception of $p = 2$. $f(2) = 1, f(p) = 0$ for $p = 3, 5, 7, 13, 23; f(p) = 3$ for $p = 11$, $17, 19, 29, 37; f(31) = f(43) = 2$ and $f(41) = 4$ yield $\Lambda^*(5, 2) = 44$.

4. The proof of Theorem 2 is essentially the proof of Lehmer and Lehmer **(3)** and R. Graham (unpublished).

(1) It suffices to prove that $\Lambda^*(2, 3) = \infty$.

Given m, let

$$f(3) = 0, \qquad f(3t + 1) = 0, \qquad f(3s + 2) = 1,$$

where $3t + 1$ and $3s + 2$ are primes $< m$. Then $f(3w + 1) = 0$ and $f(3w + 2) = 1$ for $3w + 2 < m$. Hence no three consecutive integers smaller than m can be in the same class. Therefore $\Lambda^*(2, 3) = \infty$.

(2) k even follows directly from 1. It suffices to prove $\Lambda^*(k, 4) = \infty$ for k odd.

Given m, let

$$f(2) = 1 \quad \text{and } f(2t + 1) = 0 \quad \text{for } 2t + 1 \text{ a prime.}$$

It follows that $f(4w + 1) = 0$ and $f(4w + 2) = 1$ for $4w + 2 < m$. Hence no four consecutive integers $<m$ can be in the same class. Therefore $\Lambda^*(k, w) = \infty$ for $w \geqslant 4$.

References

1. A. Brauer, *Ueber Sequenzen von Potenzresten*, Akad. der Wiss., Berlin Sitz. (1928), 9–16.
2. M. Dunton, *A bound for consecutive pairs of cubic residues* (to appear).
3. D. H. Lehmer and Emma Lehmer, *On runs of residues*, Proc. Am. Math. Soc., *13* (1962), 102–106.
4. D. H. Lehmer, E. Lehmer, and W. H. Mills, *Pairs of consecutive power residues*, Can. J. Math., *15* (1963), 172–177.
5. W. H. Mills and R. Bierstedt, *On the bound for a pair of consecutive quartic residues modulo a prime*, Proc. Am. Math. Soc., *14* (1963), 620–632.
6. W. H. Mills, *Characters with preassigned values*, Can. J. Math., *15* (1963), 169–171.

Washington State University

https://doi.org/10.4153/CJM-1964-030-6 Published online by Cambridge University Press