MATHEMATICS OF COMPUTATION, VOLUME 24, NUMBER 111, JULY, 1970

Consecutive Power Residues or Nonresidues

By J. R. Rabung and J. H. Jordan

Abstract. For any positive integers k and l, A. Brauer [1] has shown that there exists a number $z(k, l)$ such that, for any prime number $p > z(k, l)$, a sequence of l consecutive numbers occurs in at least one kth-power class modulo p. For particular k and l, one is sometimes able to find a least bound, $\Lambda^*(k, l)$, before, or at which, the first member of such a sequence must appear. In this paper, we describe a method used to compute $\Lambda^*(8, 2)$ and $\Lambda^*(3, 3)$.

Introduction. A. Brauer [1] showed in 1928 that, for any positive integers k and l, there exists a constant $z(k, l)$, such that, for each prime p with $p \geqq z(k, l)$, any kth-power character χ modulo p has the property that

$$\chi(a) = \chi(a + 1) = \chi(a + 2) = \cdots = \chi(a + l - 1), \tag{1}$$

for some integer a. We shall refer to the sequence $a, a + 1, a + 2, \cdots, a + l - 1$, in (1), as a sequence of l kth-power residues or nonresidues according as $\chi(a)$ is or is not unity. Also, for a given kth-power character χ modulo p, we shall say that an integer a belongs to kth-power class i if $\chi(a) = \rho^i$, where ρ is a fixed primitive kth root of unity. Since the structure of the kth-power classes modulo p is unaffected by the choice of χ or ρ, we may speak of integers as belonging to the same kth-power class modulo p without prior mention of a particular character or root of unity.

Let us consider the particular case of Brauer's result with $k = 4$ and $l = 2$. We have that, for all sufficiently large primes p, there must exist two consecutive integers belonging to the same fourth-power class modulo p. We ask, now, where the first such pair will occur. Since 1 is a quartic residue for any prime, the pair (1, 2) will consist of consecutive quartic residues if 2 is a quartic residue modulo p. So, we assume that 2 is a quartic nonresidue modulo p; that is, 2 belongs to quartic class 1, 2, or 3, for any given quartic character χ modulo p and a fixed primitive fourth root of unity ρ. Let us take the case $\chi(2) = \rho$, first. Then, if $\chi(3) = \rho$ or $\chi(3) = \rho^2$, we have the pair (2, 3) or (3, 4) in the same quartic class modulo p. Consider the case $\chi(3) = 1$. Here, we find that if 5 belongs to quartic class 0, 1, 2, or 3, modulo p (relative to the same χ and ρ, of course), then the pair (15, 16), (5, 6), (4, 5), or (9, 10), respectively, will appear in one of the quartic classes modulo p. So we turn to the case $\chi(3) = \rho^3$. Here, again, 5 being placed in class 0, 1, or 2, causes the consecutive pair (5, 6), (15, 16), or (4, 5) to appear in one quartic class. But $\chi(5) = \rho^3$ does not readily lead to such a pair. In this case, one need only observe that 7 cannot be found in any quartic class modulo p without causing the appearance of one of the pairs (6, 7), (14, 15), (20, 21), or (7, 8), in one quartic class. Thus, we see that, if 2 is in quartic class 0 or 1, a consecutive pair $(a, a + 1)$, with $a \leqq 20$, must occur in one class, The same applies if 2

Received August 21, 1969, revised December 1, 1969.

AMS Subject Classifications. Primary 1055, 1003.

Key Words and Phrases. kth-power character, kth-power residues, kth-power nonresidues, kth-power class.

belongs to quartic class 3, since this simply amounts to a renumbering of the cases discussed above with 2 in class 1. And, finally, if 2 is in quartic class 2 modulo p relative to some χ and ρ, then 3's appearance in class 0, 1, 2, or 3 will cause (3, 4), (8, 9), (2, 3), or (8, 9), respectively, in one class.

This discussion shows that, for any sufficiently large prime p, a pair of consecutive integers $(a, a + 1)$, with $a \leqq 20$, must occur in at least one quartic class modulo p. And the only possible primes for which such a pair may not occur will be those involved in obtaining this bound; namely, 2, 3, 5, and 7. A quick investigation shows that 2, 3, and 5 are, indeed, exceptions to the result, but that the pair (1, 2) appears in the class of quartic residues modulo 7. Also, by a theorem of W. Mills [2], there exist infinitely many primes which have a kth-power character χ assigning the values

$$\chi(2) = \rho, \qquad \chi(3) = \rho^3, \qquad \chi(5) = \rho^3, \qquad \chi(7) = \rho^2,$$

for a fixed primitive fourth root of unity ρ. This is the case which leads to the consecutive pair (20, 21) in one class, and in which no earlier pair occurs. So, $a \leqq 20$ is best possible.

Papers by M. Dunton [3] and by D. Lehmer, E. Lehmer, J. Selfridge, and W. Mills [4], and others (see [5]–[8]), first investigated this problem under the condition that $\chi(a) = 1$ in (1). In [4], the authors used the notation $\Lambda(k, l)$ to mean the greatest lower bound of the set of integers n, such that, for all but a finite numbers of primes, there is an $a \leqq n$ for which (1) holds, with $\chi(a) = 1$. Miss Dunton showed, for example, $\Lambda(3, 2) = 77$ with exceptional primes 2, 7, and 13. R. Graham [9] established that $\Lambda(k, l) = \infty$ for $l \geqq 4$.

J. Jordan [10] defined $\Lambda^*(k, l)$ similarly to $\Lambda(k, l)$ except that he omitted the requirement that $\chi(a) = 1$ in (1). That is, where the search in the above papers was for a sequence of l kth-power residues, the search in [10] was for a sequence of l kth-power residues *or* nonresidues. With this notation, the simple result displayed above is expressed $\Lambda^*(4, 2) = 20$. In addition, Jordan found:

$$\Lambda^*(2, 2) = 3 \quad \text{except for 2;}$$

$$\Lambda^*(3, 2) = 8 \quad \text{except for 2;}$$

$$\Lambda^*(4, 2) = 20 \quad \text{except for 2, 3, and 5;}$$

$$\Lambda^*(5, 2) = 44 \quad \text{except for 2;}$$

$$\Lambda^*(6, 2) = 80 \quad \text{except for 2, 3, and 7;}$$

$$\Lambda^*(7, 2) = 343 \quad \text{except for 2;}$$

$$\Lambda^*(2, 3) = \infty; \qquad \Lambda^*(k, l) = \infty \quad \text{for } l \geqq 4.$$

To this we are now able to add:

$$\Lambda^*(8, 2) = 399 \quad \text{except for 2;}$$

$$\Lambda^*(3, 3) = 2499 \quad \text{except for 2, 3, 7, 13, and 19.}$$

These last two results are too cumbersome and hazardous to approach without the aid of a computer. They were accomplished on an IBM 360 model 67. We shall give a brief description of the program used.

Method. The program was designed to handle these problems in much the same way as the simple problem of $\Lambda^*(4, 2)$ was handled in our previous remarks. That is, in seeking $\Lambda^*(k, l)$ the program placed successive prime numbers in the various kth-power classes and looked for sequences of l consecutive integers all of which occurred in the same kth-power class. If a prime could not be placed in any class without the finding of such a sequence, then a preceding prime would be placed in a class other than the one in which it had been placed. This was done until the first, say, n primes had each been placed in each of the k classes, and each placing had caused the appearance of a sequence of l consecutive integers in one class. To determine in what class an integer was, the program found the prime factorization of that integer and, providing each prime in this factorization had been previously placed, the vector dot product idea used in [4] was employed to find the desired class. The integers tested in this way were those within the reasonable vicinity of multiples of the latest prime being placed.

Once this program arrived at a bound, it attempted to place all primes up to that bound so that no sequence of l integers in the same class occurred before the bound. If this failed, the bound was lowered and the attempt was made again. Once all primes had been successfully placed up to such a bound, Mill's theorem on preassigning character values (see [2]) could be used to show the bound to be best possible, and the results were obtained.

In arriving at the bound $\Lambda^*(8, 2) \leqq 399$, the computer ran through some 971 different placements of primes. This required about 90 seconds of computer time. Of course, the number of cases was greatly reduced by the simple observation that the prime 2 is always a quadratic residue modulo a prime p of the form $8m + 1$. So, saying that the prime q lies in eighth power class i modulo p if $\chi(q) = \rho^i$, where χ is a fixed eighth power character modulo p and ρ is a fixed primitive eighth root of unity, 2 can only appear in an even-numbered eighth power class. Other observations of symmetry between certain cases helped also in keeping the number of considerations low. Once the bound 399 was obtained, it was an easy matter to show without help from the computer that it was best possible simply by placing the remaining primes less than 399 and appealing to Mill's theorem. The following indicates how the primes were placed in order that no pair of consecutive integers <399 occurred in the same eighth power class:

Class 1: 3, 89, 107, 113, 131, 149, 163, 167, 173, 197, 227, 229, 251, 257, 269, 293, 307, 311, 317, 353.

Class 2: 17, 53, 59, 71, 101, 137, 281, 389.

Class 3: 83.

Class 4: 2, 5, 11, 23, 41, 47.

Class 5: 29.

Class 7: 19.

All other primes less than 399 were placed in class 0.

Finding that $\Lambda^*(3, 3) = 2499$ was a bit more difficult. The computer here ran through 1308 different placement vectors before arriving at a bound, $\Lambda^*(3, 3) \leqq 6726$. This took about three minutes of computer time. The process of extending these original placements of primes to arrive at the best bound took another three minutes and ran through 1183 more cases. The vector which establishes our result makes the following placements of primes less than 2499:

Class 1: 3, 5, 7, 11, 23, 37, 43, 53, 59, 97, 113, 131, 149, 157, 181, 199, 211, 223, 229,

233, 241, 293, 313, 317, 347, 353, 359, 373, 383, 421, 463, 487, 499, 523, 541, 571, 601, 641, 647, 683, 701, 743, 761, 773, 797, 821, 839, 857, 881, 887, 911, 941, 947, 991, 1063, 1087, 1093, 1097, 1123, 1129, 1171, 1213, 1231, 1249, 1303, 1321, 1399, 1667, 1697, 1709, 1723, 1787, 1811, 1847, 1871, 1877, 1889, 1901, 1913, 1949, 1979, 2029, 2063, 2081, 2099, 2153, 2237, 2371, 2393, 2437, 2447.

Class 2: 19, 29, 71, 83, 103, 109, 137, 167, 173, 191, 197, 271, 277, 311, 389, 401, 419, 479, 547, 613, 673, 691, 809, 929, 971, 1153, 2351.

The rest of the primes less than 2499 are placed in class 0.

We are indebted to the computation centers at both Washington State University and Pennsylvania State University for the use of their facilities.

Mathematics Research Center
Naval Research Laboratory
Washington, D. C. 20390

Department of Mathematics
Washington State University
Pullman, Washington 99163

1. A. BRAUER, "Über Sequenzen von Potenzresten," *S.-B. Preuss. Akad. Wiss. Phys.-Math. Kl.*, v. 1928, pp. 9–16.

2. W. MILLS, "Characters with preassigned values," *Canad. J. Math.*, v. 15, 1963, pp. 169–171. MR. **28** # 71.

3. M. DUNTON, "Bounds for pairs of cubic residues," *Proc. Amer. Math. Soc.*, v. 16, 1965, pp. 330–332. MR **30** #3055.

4. D. LEHMER, E. LEHMER, W. MILLS & J. SELFRIDGE, "Machine proof of a theorem on cubic residues," *Math. Comp.*, v. 16, 1962, pp. 407–415. MR **28** #5578.

5. D. LEHMER & E. LEHMER, "On runs of residues," *Proc. Amer. Math. Soc.*, v. 13, 1962, pp. 102–106. MR. **25** #2025.

6. D. LEHMER, E. LEHMER & W. MILLS, "Pairs of consecutive power residues," *Canad. J. Math.*, v. 15, 1963, pp. 172–177. MR **26** #3660.

7. W. MILLS & R. BIERSTEDT, "On the bound for a pair of consecutive quartic residues modulo a prime *p*," *Proc. Amer. Math. Soc.*, v. 14, 1963, pp. 628–632.

8. J. BRILLHART, D. LEHMER & E. LEHMER, "Bounds for pairs of consecutive seventh and higher power residues," *Math. Comp.*, v. 18, 1964, pp. 397–407. MR **29** #2214.

9. R. L. GRAHAM, "On quadruples of consecutive *k*th power residues," *Proc. Amer. Math. Soc.*, v. 15, 1964, pp. 196–197. MR. **28** #2078.

10. J. JORDAN, "Pairs of consecutive power residues or non-residues," *Canad. J. Math.*, v. 16, 1964, pp. 310–314. MR **28** #5028.