PAIRS OF CONSECUTIVE POWER RESIDUES

D. H. LEHMER, EMMA LEHMER, AND W. H. MILLS

Introduction. Until recently none of the numerous papers on the distribution of quadratic and higher power residues was concerned with questions of the following sort: Let k and m be positive integers. According to a theorem of Brauer **(1)**, for every sufficiently large prime p there exist m consecutive positive integers $r, r+1, \ldots, r+m-1$, each of which is a kth power residue of p. Let $r(k, m, p)$ denote the least such r. What can be said about the behaviour of $r(k, m, p)$ as p varies? In particular, for what values of k and m is $r(k, m, p)$ bounded, and for these values what is its maximum? For a fixed k and m we call a prime exceptional and denote it by p^* if there do not exist m consecutive integers each of which is a kth power residue of p^*. Set $\Lambda(k, m) = \operatorname{Max} r(k, m, p)$, where the maximum is taken over all non-exceptional primes p. In a previous paper **(4)** Lehmer and Lehmer showed that

$$\Lambda(k, m) = \infty \begin{cases} \text{if } k \text{ is even and } m \geqslant 3, \\ \text{if } 2 < k \leqslant 1048909 \text{ and } m \geqslant 4. \end{cases} \tag{1}$$

If $\Lambda(k, m)$ is finite it follows from Theorem 2 of the preceding paper that there is an infinity of primes p such that $r(k, m, p) = \Lambda(k, m)$.

In this paper we discuss $\Lambda(k, 2)$ for $k \leqslant 6$. The question of whether $\Lambda(k, 2)$ is finite for all k is a very interesting open question. To summarize we cite the following results:

$$\Lambda(2, 2) = 9, \qquad p^* = 2, 3, 5, \tag{2}$$

$$\Lambda(3, 2) = 77, \qquad p^* = 2, 7, 13 \quad \text{(M. Dunton)}, \tag{3}$$

$$\Lambda(4, 2) = 1224, \qquad p^* = 2, 3, 5, 13, 17, 41 \quad \text{(W. H. Mills and R. Bierstedt)}, \tag{4}$$

$$\Lambda(5, 2) = 7888, \qquad p^* = 2, 11, 41, 71, 101, \tag{5}$$

$$\Lambda(6, 2) = 202124, \quad p^* = 2, 3, 5, 7, 13, 19, 43, 61, 97, 157, 277. \tag{6}$$

Result (6), for example, states that every prime $p > 277$ has two consecutive numbers which are sextic residues and do not exceed 202125. Furthermore, this limit is best possible because there are infinitely many primes having (202124, 202125) as the least pair of consecutive sextic residues.

Result (2) is easily verified by discussing the cases in which 2 and 5 are or are not quadratic residues of p. On the other hand any prime, like 43, for which 2, 3, 5, and 7 are all quadratic non-residues, will have (9, 10) as the least pair

Received January 19, 1962.

of consecutive quadratic residues. The corresponding result (3) for cubic residues was obtained by Dunton **(2)** by a similar argument involving more cases. It was this result that aroused our interest in the whole problem of $\Lambda(k, m)$. Result (4) for quartic residues was obtained independently by Mills and Bierstedt **(6)** by considering more than 100 cases. Results (5) and (6) are new and were made possible by electronic computers, not only in the preparation of the necessary data for the proofs, but in the actual carrying out of the logical steps in the proofs themselves. Result (5) could have conceivably been obtained by hand computation, although it required the consideration of 4568 cases. However, the proof of (6) which required the consideration of 25411 cases would have been impractical without the use of high speed computers, at least by our present methods. Since we cannot give the full details of the machine's steps in the proofs of these results we content ourselves with giving the theoretical background and some aspects of the machine programme.

The calculations were made at the University of California Computer Center in Berkeley on the IBM 701 and 704 computers. In a future paper **(5)** having to do with the determination of $\Lambda(3, 3)$ (which equals 23532) we plan to give more of the computational details.

1. Preliminary considerations. Let p be a prime, $p = kx + 1$, and let ind n denote the index of n with respect to some primitive root g of p, that is,

$$g^{\text{ind } n} \equiv n \pmod{p}.$$

Let $R(n)$ denote the integer valued function defined by

$$R(n) \equiv \text{ind } n \pmod{k},\ 0 \leqslant R(n) < k,$$

for every integer n not divisible by p. Clearly n is a kth power residue of p if and only if $R(n) = 0$. For machine purposes the function $R(n)$ is more convenient than the multiplicative complex-valued character function. Let

$$S:\quad q_1 < q_2 < \ldots < q_t$$

be a finite set of distinct primes. The vector

$$[R(q_1), R(q_2), \ldots, R(q_t)] \tag{7}$$

will be called an S-vector. Let n be any number of the form

$$n = q_1^{\alpha_1} q_2^{\alpha_2} \ldots q_t^{\alpha_t}, \tag{8}$$

where the α_i are non-negative integers. Let a_i be the least non-negative residue of α_i modulo k. The vector

$$[a_1, a_2, \ldots, a_t] \tag{9}$$

will be called the decomposition vector of n. From the additive properties of the index we have

$$R(n) \equiv a_1 R(q_1) + \ldots + a_t R(q_t) \pmod{k}.$$

Thus n is a kth power residue of p if and only if

$$a_1R(q_1) + a_2R(q_2) + \ldots + a_tR(q_t) \equiv 0 \pmod{k},$$

or, as one could say, if and only if the vectors (7) and (9) are *orthogonal modulo* k or simply *k-orthogonal.*

It is clear that to each prime p not in the set S, there corresponds an S-vector. Conversely every vector $[r_1, r_2, \ldots, r_t]$, $0 \leqslant r_i < k$, that satisfies certain parity conditions is the S-vector of infinitely many primes. (See Theorem 3 of the preceding paper.) Thus all primes not in S are sorted into k^t compartments by assigning values to each of the components in the S-vector. Thus we can hope to prove a result about the infinitude of primes not in S by merely considering a finite number of S-vectors. In particular $\Lambda(k, 2) < L$ if for each S-vector V there exist a pair of consecutive positive integers not exceeding L, both of the form (8), whose corresponding decomposition vectors (9) are both k-orthogonal to V. For this to work there must be an adequate supply of pairs of consecutive positive integers of the form (8). By a crude probabilistic argument one may expect s pairs to be adequate, where

$$s = -t \log k/[\log(1 - k^{-2})].$$

In actual practice we used $t = 22$. For $t = 22$ and $k = 5$ and 6, this formula gives $s = 867$ and 1400 respectively. We used 1020 and 2398 respectively.

However, the numbers (8) whose primes factors are restricted to the given finite set S are relatively scarce, and pairs of consecutive integers of this kind are scarcer still. In fact Störmer **(7)** has shown that the total number of such pairs is finite.* To obtain as many pairs as possible we usually took S to be the set of the first t primes. For the problems under consideration we had to find all such pairs below a fixed limit L. Such a list can be prepared on a high speed computer in any one of several straightforward ways (see **(5)**).

After such a list is prepared, we produce the decomposition vectors of the two elements of each pair. By the *k-dimension* of a number n with decomposition vector $[a_1, a_2, \ldots, a_t]$ we mean the largest d such that $a_d \neq 0$. The k-dimension of a kth power is defined to be zero. By the *k-dimension* of a pair $(n, n + 1)$ we mean the larger k-dimension of the two numbers. The next step is to sort the pairs according to their k-dimensions. We now have for each $d \leqslant t$ a set of pairs of decomposition vectors. For example, for $k = 5$, $d = 6$, and S the set of the first six primes, the smallest pair is (12, 13) whose decomposition vectors are [2, 1, 0, 0, 0, 0], [0, 0, 0, 0, 0, 1] and the largest pair is

$$123200 = 2^6 \cdot 5^2 \cdot 7 \cdot 11, \quad 123201 = 3^6 \cdot 13^2$$

*By a modification of Störmer's method Lehmer **(3)** was able to show that there are less than $\frac{1}{2}(q_t + 1)(2^t - 1)$ such pairs. He determined all such pairs for the set S consisting of the first 13 primes. The determination of *all* such pairs corresponding to a set with more than 13 primes becomes prohibitive at the present time.

whose corresponding decomposition vectors are [1, 0, 2, 1, 1, 0] and [0, 1, 0, 0, 0, 2].

2. The main programme. The number t of primes needed is so large that it is not feasible to consider k^t separate cases. Hence we introduce the concept of a case vector as follows: A case vector is a vector $[a_1, a_2, \ldots, a_d]$, where a_i are integers, $0 \leqslant a_i < k$ and $d \leqslant t$. We call d the dimension of the case vector. We say that a prime p is *covered* by this case vector if $R(q_i) = a_i$ for $1 \leqslant i \leqslant d$.

We are now in a position to consider the main programme. First the sets of pairs of decomposition vectors are stored in the memory of the computer. The machine now proceeds to dispose of a sequence of case vectors in a methodical way described below:

Suppose that at a certain stage of the proof, the case vector is

$$A = [a_1, a_2, \ldots, a_d] \tag{10}$$

of dimension d. The machine goes through the list of pairs of k-dimension d to see if for some pair both decomposition vectors are k-orthogonal to the current case vector. If such a pair is discovered then the primes covered by (10) have a pair of consecutive kth power residues less than L. In this case if $a_1 = a_2 = \ldots = a_d = k - 1$, then the process is complete and the machine stops. Otherwise A is replaced by σA, where

$$\sigma A = \begin{cases} [a_1, a_2, \ldots, a_d + 1] \text{ if } a_d < k - 1, \\ [a_1, a_2, \ldots, a_r + 1] \text{ if } a_r < k - 1, a_{r+1} = \ldots = a_d = k - 1. \end{cases}$$

If, on the other hand, no suitable pair is discovered with k-dimension d, and if $d < t$, then A is replaced by $[a_1, a_2, \ldots, a_d, 0]$, which has dimension $d + 1$. If $d = t$ and no suitable pair is discovered, then we have an S-vector which cannot be handled with the pairs at the machine's disposal. In this case the machine puts out this S-vector, and returns to consider the next case vector in order.

3. The case $k = 5$. We now give a brief account of the proof that $\Lambda(5, 2) = 7888$. Primes p for which 2 is a quintic residue obviously have the pair (1, 2) of consecutive quintic residues. Hence we may suppose that $R(q_1) \neq 0$, $q_1 = 2$. However, because the primitive root g can be replaced by any other primitive root of the prime p, we can suppose that $R(q_1) = 4$. Thus we need to consider only the case vectors whose first component is 4, and in particular the first case vector is [4] with $d = 1$.

It is known from cyclotomy that $p^* = 2, 11, 41, 71$, and 101 are the only exceptional primes. It is clear that if these primes are not included in the set S, then there is bound to be an output of S-vectors which the machine cannot handle, namely the S-vectors of these primes. In the actual run we took

$t = 22$, with S the set of the first 21 primes and 101. Four runs were actually made, the first two with $L = 2^{15}$ and 2^{13} respectively produced no output, the third with $L = 2^{12}$ produced output of the form

$$[4, 0, 0, 4, 4, 3, 4, 3, 3, 0, \ldots]. \tag{11}$$

All this output is disposed of by the pair

$$7888 = 2^4 \cdot 17 \cdot 29, \quad 7889 = 7^3 \cdot 23.$$

A final run was made with $L = 7889$ with no output. Hence $\Lambda(5, 2) \leqslant 7888$. Each of these four runs took about 3 minutes. As a check on the work the machine was programmed to report the disposal of every case vector of the maximal dimension $d = 22$. The machine reported handling successfully the 5 expected case vectors

$$[4, 1, 1, 1, 2, 4, 0, 4, 4, 4, 1, 4, 0, 3, 2, 2, 1, 3, 4, 1, 4, a], \ (a = 0, 1, 2, 3, 4),$$

the first 21 components of which correspond to the quintic characters of the first 21 primes modulo 101. Had no provision been made for the exceptional prime 101, that is, had S consisted of the first 22 primes, the machine would have reported that it could not dispose of the vector

$$[4, 1, 1, 1, 2, 4, 0, 4, 4, 4, 1, 4, 0, 3, 2, 2, 1, 3, 4, 1, 4, 1],$$

the last component of which corresponds to the character of 79 modulo 101.

In the final run the machine disposed of 4568 different cases.

It now remains to show that there exist primes p whose least pair of consecutive quintic residues is (7888, 7889). It is clear that the quintic characters of the small primes modulo such p are given by (11). Thus our problem is to extend the vector (11) to the set of all primes below 7888. It can be shown that any prime p such that

$$\begin{cases} R(3) = R(5) = R(29) = 0 \\ R(13) = R(19) = R(23) = R(31) = R(41) = R(43) = R(211) \\ \qquad\qquad = R(277) = 3 \\ R(q) = 4 \text{ for all other primes } q \text{ with } 2 \leqslant q < 7888 \end{cases} \tag{12}$$

actually has the desired property that the least positive integer n for which $R(n) = R(n + 1) = 0$ is $n = 7888$. There are several good ways in which this can be checked by machine. In actual practice we did this both by machine and by inspection of factor tables. By Kummer's theorem (see preceding paper) there exist an infinity of primes p satisfying (12). Hence $\Lambda(5, 2) = 7888$.

4. The case $k = 6$. By a similar, but more complicated procedure we were able to determine $\Lambda(6, 2)$. The final run with $L = 202125$ involved the consideration of 25411 case vectors, and was completed in 18 minutes. A set of primes for which (202124, 202125) is the least pair of consecutive sextic residues is characterized by

$$(13)\quad \begin{cases} R(3) = R(43) = R(61) = 0, \\ R(71) = R(101) = R(331) = R(733) = R(1423) = R(4877) \\ \qquad = R(5413) = R(6043) = 4, \\ R(q) = 5 \text{ for all other primes } q \text{ such that } 2 \leqslant q \leqslant 202123. \end{cases}$$

By Theorem 3 of the preceding paper there exist an infinite number of such primes p. Thus we established that

$$\Lambda(6, 2) = 202124.$$

The problem of exhibiting a prime characterized by (12) or (13) is a sieve problem beyond the capabilities of existing electronic computers.

Added in proof. R. Graham has recently shown that $\Lambda(k, 4) = \infty$ for $k > 1$.

References

1. Alfred 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, *On a problem of Störmer* (to appear in Illinois J. Math.).
4. D. H. Lehmer and Emma Lehmer, *On runs of residues*, Proc. Amer. Math. Soc., *13* (1962), 102–106.
5. D. H. Lehmer and Emma Lehmer, W. H. Mills, and J. L. Selfridge, *Machine proof of a theorem on cubic residues* (to appear in Math. of Computation).
6. W. H. Mills and R. Bierstedt, *On the bound for a pair of consecutive quartic residues modulo a prime* (to appear in Proc. Amer. Math. Soc.).
7. Carl Störmer, *Quelques théorèmes sur l'équation de Pell et leurs applications*, Vidensk Selskabs., Christiania Skrifter, I. Math.-nat. Kl., no. 2 (1897), 1–48.

University of California, Berkeley
Yale University