ON RUNS OF RESIDUES[1]

D. H. LEHMER AND EMMA LEHMER

According to a theorem of Alfred Brauer [1] all sufficiently large primes have runs of l consecutive integers that are kth power residues, where k and l are arbitrarily given integers. In this paper we consider the question of the first appearance of such runs.

Let p be a sufficiently large prime and let

$$r = r(k, l, p)$$

be the least positive integer such that

$$(1) \qquad r, \quad r+1, \quad r+2, \cdots, \quad r+l-1$$

are all congruent modulo p to kth powers of integers >0. It is natural to ask, when k and l are given, how large is this minimum r and are there primes p for which r is arbitrarily large? If we let

$$\Lambda(k, l) = \limsup_{p\to\infty} r(k, l, p)$$

then is Λ infinite or finite, and if finite what is its value?

It is easy to see that

$$\Lambda(2, 2) = 9$$

so that every prime $p > 5$ has a pair of consecutive quadratic residues which appears not later than the pair (9, 10). In fact if 10 is not a quadratic residue of p then either 2 or 5 is, and so we have either (1, 2) or (4, 5) as a pair of consecutive residues.

By an elaboration of this reasoning M. Dunton has shown that

$$\Lambda(3, 2) = 77,$$

and more recently W. H. Mills has shown that

$$\Lambda(4, 2) = 1224.$$

Both of these proofs are as yet unpublished.

In contrast to these results we prove in this paper that

$$(2) \qquad \Lambda(2, 3) = \infty,$$

and

Presented to the Society, November 19, 1960 under the title *On the distribution of consecutive quadratic and cubic residues*; received by the editors December 5, 1960.

[1] This paper is the result of unsupported research.

$$\Lambda(k, 4) = \infty, \qquad k \leqq 1048909. \tag{3}$$

In other words, by proper choice of p *the appearance of a run of* 3 *quadratic residues or of* 4 *higher residues can be postponed as long as desired.*

PROOF OF (2). Let N be a positive integer. Then it suffices to prove that there is a prime p for which

$$r(2, 3, p) > N. \tag{4}$$

Let

$$q_1, q_2, \cdots, q_t$$

be all the primes $\leqq N$.

By the quadratic reciprocity law, those primes which have a particular prime q_i as a quadratic residue belong to a set of arithmetic progressions of common difference $4q_i$. Those primes which have q_i for a nonresidue likewise belong to another set of arithmetic progressions of difference $4q_i$. If we combine the progressions of the first kind for every prime $q_i \equiv 1 \pmod 3$ with those of the second kind for every prime $q_i \equiv 2 \pmod 3$ and use Dirichlet's theorem on primes in arithmetic progressions we see that there exists a prime p such that

$$\left(\frac{q}{p}\right) \equiv q \pmod 3 \qquad (q \neq 3, q \leqq N).$$

Using the multiplicative property of Legendre's symbol we see that

$$\left(\frac{m}{p}\right) \equiv m \pmod 3 \qquad (m \not\equiv 0 \pmod 3, m \leqq N). \tag{5}$$

But among any three consecutive numbers $\leqq N$ there is one congruent to $-1 \pmod 3$ and hence, by (5), is a nonresidue of this prime p. Hence the first run of three consecutive quadratic residues lies beyond N. This proves (4) and (2).

PROOF OF (3). The following theorem enables one to prove that for $l \geqq 4$, $\Lambda(k, l) = \infty$ for all k up to high limits. It is clear that for such a program one may confine k to odd prime values and take $l = 4$.

THEOREM A. *Let k and $p^* = kn+1$ be odd primes. Suppose further that* 2 *is not a kth power residue of p^*, and p^* is small enough so that it has no run of* 4 *consecutive kth power residues. Then $\Lambda(k, 4) = \infty$.*

For the proof we need the following lemma which is a special case of a theorem of Kummer [2].

LEMMA. *Let k be an odd prime and $q_1, q_2, \cdots, q_t$ be any set of distinct primes different from k. Let $\gamma_1, \gamma_2, \cdots, \gamma_t$ be a set of kth roots of unity. Then there exist infinitely many primes $p \equiv 1 \pmod{k}$ with corresponding kth power character χ modulo p such that*

$$\chi(q_i) = \gamma_i \qquad (i = 1(1)t).$$

To prove the theorem let N be an arbitrarily large integer and let $q_1, q_2, \cdots, q_t$ be the primes $\leqq N$ with the exception of the prime p^*. Choosing a nonprincipal character, let γ_i be the kth power character of q_i modulo p^*. By the lemma there exist infinitely many primes $p \equiv 1 \pmod{k}$ such that the q's have the same characters modulo p as modulo p^*. By the multiplicative property of characters this will be true of all the integers $m \leqq N$ that are not divisible by p^*. Hence p has no run of 4 consecutive residues $\leqq N$ unless one of these residues is a multiple of p^*. But two units on either side of this multiple of p^* we find numbers congruent to $\pm 2 \pmod{p^*}$ which are nonresidues of p^* and hence of p. Hence there is also no run of 4 residues which includes a multiple of $p^* \leqq N$. This proves the theorem.

The fact that $\Lambda(3, 4) = \infty$ follows from the theorem by setting $k=3$ and $p^*=7$. Similarly by taking $k=5$ and $p^*=11$ we have $\Lambda(5, 4) = \infty$.

There is good reason to believe that $\Lambda(k, 4) = \infty$ for all k. To prove this it would suffice to prove for each prime k the existence of a prime $p^* = kn+1$ satisfying the hypothesis of the theorem. If n is not too large, then $p^* = kn+1$ will not have 4 consecutive kth power residues. In fact n is precisely the number of residues altogether. Trivially, if $n=2$ we have $\Lambda(k, 4) = \infty$ as with $k=3, 5, 11, 23$, etc. With a little more effort we can prove

THEOREM B. *If $n \leqq 12$ then $\Lambda(k, 4) = \infty$.*

PROOF. We may suppose that $k > 5$. Let $p^* = kn+1$ be a prime not satisfying the hypothesis of Theorem A. This failure is not due to the fact that 2 is a residue of p^*. In fact if 2 were a residue, p^* would divide $2^n - 1$ by Euler's criterion. Since n is even and $\leqq 12$ this restricts p^* to the values

$$3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 31.$$

In each case the corresponding value of k is $\leqq 5$. Hence 2 must be a nonresidue along with -2 and $(p \pm 1)/2$. Hence we may suppose that p^* has a run of 4 residues

$$2 < a,\ a+1,\ a+2,\ a+3 < (p-1)/2$$

as well as the negatives of these modulo p^*. Besides these 8 residues there are the two residues congruent to $\pm(a+2)/a \not\equiv \pm 1$. These two are isolated since

$$\frac{a+2}{a} - 1 = \frac{2}{a} \quad \text{and} \quad \frac{a+2}{a} + 1 = \frac{2}{a}(a+1)$$

are obvious nonresidues. The reciprocals $\pm a/(a+2)$ are also isolated residues and they are new because

$$\frac{a+2}{a} \equiv -\frac{a}{a+2} \pmod{p^*}$$

implies

$$a(a+2) \equiv -2 \pmod{p^*}$$

in which a product of two residues is congruent to a nonresidue. Including the residues ± 1 we have accounted for at least 14 distinct kth power residues of p^*. Hence $14 \leqq n \leqq 12$, a contradiction. Therefore p^* must satisfy the hypothesis of Theorem A and so $\Lambda(k, 4) = \infty$.

A more elaborate argument involving the factors of $3^n - 1$ and the Fibonacci numbers yields a theorem in which the 12 in Theorem B is replaced by 36.

Let $p_0 = kn_0 + 1$ be the least prime congruent to 1 modulo k. Primes k for which $n_0(k) \geqq 38$ are relatively rare, only about 3% of all the primes < 50000 by actual count. The least such prime is $k = 1637$ with $n_0 = 38$, and the largest value for n_0 for primes less than 50000 is $n_0 = 80$ for $k = 47303$. The values of $k < 50000$ were calculated on the SWAC and were tested on the 7090 by John Selfridge for pairs of consecutive kth power residues. It was discovered that in this range the only pairs are the trivial pairs $(\omega, \omega + 1)$ and $(\omega^2 \equiv p - \omega - 1, \omega^2 + 1 \equiv p - \omega)$, which appear whenever n_0 is a multiple of six. Since such pairs cannot obviously combine to make a quadruplet they were eliminated from the next run, made entirely on the 7090 by John Selfridge, for $k \leqq 1048909$ in which no nontrivial pairs occurred. The largest value of $n_0 = 156$ occurred for $k = 707467$. These numerical results for which we are very grateful enable us to state the following theorem, using Theorem A.

THEOREM C. *If* $k \leqq 1048909$, *then* $\Lambda(k, 4) = \infty$.

More generally one can ask about the first appearance of l consecutive numbers each with specified kth power character modulo $p = kn + 1$, excluding of course the case already considered in which all the numbers are kth power residues. This seemingly more difficult problem is unexpectedly simple. Regardless of l the first appearance of such a set of consecutive numbers may be delayed indefinitely by proper choice of p. In fact if we set all the γ's in the lemma at 1 we can find primes p having all the primes $\leqq N$ and hence all the numbers $\leqq N$ as kth power residues. Hence if the specified characters contain as much as a single nonresidue the first appearance can be made to occur beyond N.

In a future paper, written jointly with W. H. Mills, we determine the finite numbers $\Lambda(5, 2)$, $\Lambda(6, 2)$ and $\Lambda(3, 3)$.

References

1. Alfred Brauer, *Über Sequenzen von Potenzresten*, S.-B. Deutsch. Akad. Wiss. Berlin **1928**, 9–16.

2. D. Hilbert, *Die Theorie der algebraischen Zahlkörper*, Jber. Deutsch. Math. Verein. **4** (1897), 426.

University of California, Berkeley