Bounds for Pairs of Consecutive Seventh and Higher Power Residues

By John Brillhart, D. H. Lehmer, and Emma Lehmer

Introduction. In previous papers [1], [3], [4] and [5] the first occurrence of two consecutive kth power residues of a prime p was discussed for $k = 2, 3, 4, 5$, and 6. The present paper is concerned with the same problem for $k > 6$. Before giving the results of this investigation in detail we need to recall some definitions and notations.

Let k be an integer > 1, and let $p = km + 1$ be a prime.

Let g be a primitive root of p and let $g^{\text{ind } x} \equiv x \pmod{p}$.

Let $R(n) \equiv \text{ind } n \pmod{k}$, $0 \leqq R(n) < k$. [In particular n is a kth power residue if and only if $R(n) = 0$.]

Let $r = r(k, p)$ denote the least positive r such that r and $r + 1$ are both kth powers modulo p, so that $R(r) = R(r + 1) = 0$.

Let a prime $p^* = p^*(k)$ for which no r exists be called an "exceptional prime."

Let $\Lambda(k) = \max r(k, p)$ taken over all nonexceptional primes p.

Let any vector whose components are non-negative integers less than k be called a "case vector."

For $k < 8$, to each case vector $[c_1, c_2, \cdots, c_t]$ there corresponds an infinite class of primes p for which

$$R(2) = c_1, R(3) = c_2, \cdots, R(q_t) = c_t$$

where q_t is the tth prime [6].

A case vector $[R(2), R(3), \cdots, R(q_t)]$ characterizing an infinite class of primes for which $r(k, p) = \Lambda(k)$ will be called a "maximal case vector."

1. Results. For convenience of reference new and old results are given in Table I. Previous results are recognized by references in square brackets.

TABLE I

k	$\Lambda(k)$	Exceptional primes $p^*(k)$	References
2	9	3, 5	[2]
3	77	7, 13	[1]
4	1224	5, 13, 17, 41	[5]
5	7888	11, 41, 71, 101	[3]
6	202124	7, 13, 19, 43, 61, 97, 157, 277	[3]
7	1649375	29, 71, 113, 491	
8	$\geqq 1200744$	17, 41, 113	
9	$> 10^7$	19, 37, 73, 181, 523, 577	
10	$\geqq 22458303$	11, 31, 41, 71, 101, 281, 401, 1181	

Received September 30, 1963. Revised November 7, 1963.

If $k > 9$ and either odd or twice an odd prime of the form $4n + 3$, then $\Lambda(k) > 5^k$.

In Table II we give maximal case vectors for $k < 8$.

TABLE II

k	Description of maximal case vector	References
2	$R(q) = R(2) = 1$ for all primes $q < 9$	[2]
3	$R(5) = 0, R(q) = 2$ for $q = 7, 19$ $R(q) = 1$ for all other primes $q < 77$	[1]
4	$R(3) = 0, R(q) = 1$ for all other primes $q < 1224$	[5]
5	$R(q) = 0$ for $q = 3, 5, 29$ $R(q) = 2$ for $q = 13, 19, 23, 31, 41, 43,$ $211, 277, R(q) = 1$ for all other primes $q < 7888$	[3]
6	$R(q) = 0$ for $q = 3, 43, 61$ $R(q) = 2$ for $q = 71, 101, 331, 733,$ $1423, 4877, 5413, 6043$ $R(q) = 1$ for all other primes $q < 202124$	[3]
7	$R(q) = 0$ for $q = 3, 41$ $R(q) = 2$ for $q = 79, 137, 197, 233,$ $269, 277, 463, 467, 797, 1709, 2647, 2903, 15791$ $R(q) = 1$ for all other primes $q < 1649375$	

In order to avoid repetition, the reader is referred to the previous papers [3] and [4] for a description of general methods of machine proof.

2. The Case $k = 7$. By inspection of the values of $\Lambda(k)$ for $k = 3$ and 5 it seemed plausible that $\Lambda(7)$ might be less than 10^7. Therefore an exploratory run, using a program similar to that used for $k = 5$ and 6, was made with dimension $d = 22$ and limit $L = 10^7$. All 4935 pairs $(n, n + 1)$ whose prime factors are restricted to the first 22 primes were computed and condensed (as in [3]) to form the set of trial vectors

$$A = [a_1, a_2, \cdots, a_d]$$

in which each a_i is the exponent of q_i in $n = \prod q_i^{\alpha_i}$ modulo 7. Since we are interested only in primes having 2 for a seventh power nonresidue, and since the nonresidue classes are interchangeable, the case vector was started at [1, 0] and stopped at [2, 0]. Between these limits the machine examined only 1179741 cases, rather than the total number of 7^{21} cases. Fortunately the machine was able to settle 95 per cent

of the cases with vectors of dimension $d \leqq 12$. Beyond $d = 12$ there is a sharp drop in the number of cases, as can be seen from Table III.

TABLE III

d	No. of cases settled	d	No. of cases settled	d	No. of cases settled
2	0	9	211167	16	140
3	4	10	330811	17	85
4	56	11	315639	18	80
5	494	12	163367	19	66
6	3820	13	42502	20	70
7	20524	14	6593	21	41
8	83661	15	573	22	48

This slow preliminary run took 206 minutes and left 8 cases undecided. These were the 7 case vectors starting with

$$[1, 3, 4, 3, 5, 3, 1, 3, 4, 1, 3]$$

and the case vector

$$[1, 5, 5, 4, 1, 3, 4, 1, 1, 4, 1, 3, 0, 3, 3, 2, 5, 2, 5, 2, 3, 5].$$

Actually these exceptional vectors were expected in advance since they correspond to the characters of the exceptional primes $p^* = 113$ and 491. These vectors can readily be eliminated by hand using small multiples of the corresponding exceptional primes as follows:

$R(113)$	Pair of 7th power residues	
0	113	$114 = 2\cdot3\cdot19$
1	$2260 = 2^2\cdot5\cdot113$	$2261 = 7\cdot17\cdot19$
2	$1130 = 2\cdot5\cdot113$	$1131 = 3\cdot13\cdot29$
3	$1581 = 3\cdot17\cdot31$	$1582 = 2\cdot7\cdot113$
4	$339 = 3\cdot113$	$340 = 2^2\cdot5\cdot17$
5	$6554 = 2\cdot29\cdot113$	$6555 = 3\cdot5\cdot19\cdot23$
6	$225 = 3^2\cdot5^2$	$226 = 2\cdot113.$

Similarly

$R(491)$	Pair of 7th power residues	
0	$490 = 2\cdot5\cdot7^2$	491
1	$2945 = 5\cdot19\cdot31$	$2946 = 2\cdot3\cdot491$
2	$1472 = 2^6\cdot23$	$1473 = 3\cdot491$
3	$12765 = 3\cdot5\cdot23\cdot37$	$12766 = 2\cdot13\cdot491$
4	$3927 = 3\cdot7\cdot11\cdot17$	$3928 = 2^3\cdot491$
5	$23568 = 2^4\cdot3\cdot491$	$23569 = 7^2\cdot13\cdot37$
6	$5400 = 2^3\cdot3^3\cdot5^2$	$5401 = 11\cdot491.$

Having eliminated these exceptions we could now assert that $\Lambda(7) < 10^7$ and that there were no exceptional primes greater than 491. As a matter of fact, the only primes having no pair of consecutive 7th power residues are 29, 71, 113, 491. This fact can also be derived from the consideration of cyclotomic numbers [7].

Before proceeding to sharpen the above limit $L = 10^7$, it seemed advisable to get some idea of the true limit by trying to discover a maximal vector. It seemed likely from previous results given in Table II that a maximal vector would again be of the form

$$[1, 0, 1, 1, \cdots]$$

with most of its components equal to 1. A routine called "case test," explained in §4, was therefore written for this purpose.

Starting with the vector for which

$$R(3) = 0, R(q) = 1 \text{ for all } q \neq 3,$$

this routine soon discovered that the pair ($6560 = 2^5 \cdot 5 \cdot 41$, $6561 = 3^8$) implies $R(41) = 1$ is not a good choice for a maximal vector; neither is $R(41) = 2$ because of the pair ($284375 = 5^5 \cdot 7 \cdot 13$, $284376 = 2^3 \cdot 3 \cdot 17^2 \cdot 41$). The machine then set $R(41) = 0$, and inspected all multiples of 41 as explained in §4. Continuing this run, the machine changed $R(q)$ from 1 to 2 for the following primes:

$q = 79, 139, 197, 233, 269, 277, 463, 467, 709, 797, 1217, 1709, 2647, 2903, 15791.$*

The largest pair ($1649375 = 5^4 \cdot 7 \cdot 13 \cdot 29$, $1649376 = 2^5 \cdot 3^3 \cdot 23 \cdot 83$) caused the machine to change $R(83)$ to 2, but this choice leads to the pair

$$(259375 = 5^5 \cdot 83, 259376 = 2^4 \cdot 13 \cdot 29 \cdot 43),$$

while the choice $R(83) = 0$ leads to the pair ($10208 = 2^5 \cdot 11 \cdot 29$, $10209 = 3 \cdot 41 \cdot 83$).

Accordingly a new main run was made with $L = 1649375$, $d = 22$, and the truncation feature at $d = 6$ described in §3. This run took only 28 minutes and reported the following vectors:

$$A = [1, 0, 0, 1, 1, 1], \qquad B = [1, 0, 1, 1, 1, 1],$$

$$C = [1, 3, 4, 3, 5, 3], \qquad D = [1, 5, 5, 4, 1, 3]$$

and various tallies. We recognize the last two vectors as those corresponding to $p^* = 113$ and 491. These four vectors indicate four gaps in the proof tree, the second gap containing our proposed maximal vector. To explore the first gap the case test routine was run beginning with the vector for which $R(3) = R(5) = 0$ and $R(q) = 1$ for all other primes. This run was not able to proceed beyond the limit 1349698, so that it seemed fairly certain that $L = 1649375$ is indeed the true limit $\Lambda(7)$. Three short final runs were made with the main routine with $d \leqq 28$. One over the region [1, 0, 0, 0, 0, 0] to [1, 1, 0, 0, 0, 0] took 35 minutes and produced no output. The other two runs, over the gaps determined by vectors C and D, produced only the predicted output. Hence $\Lambda(7) = 1649375$.

* If we replace 139 by 137, then we can delete 709, 1217 to give the maximal vector quoted in Table II above.

3. Description of the Main Program. The so-called "main program" is the highly ramified proof that $\Lambda(k)$ is less than some preassigned limit L. The details of the main program, as previously coded, are given in [3] and [4]. For $k = 7$ the runs become too lengthy, especially as L approaches the true value of $\Lambda(k)$ causing the ramification to increase. For the possible benefit of anyone who might want to repeat or extend the present proof for $k \geqq 7$, we give a brief account of a new main program, faster than the old one by an order of magnitude.

As explained in [3], the proof tree is described at each point by a case vector

$$[R(q_1), R(q_2), \cdots, R(q_d)] \tag{1}$$

of dimension d whose components $R(q_i)$ are integers satisfying

$$0 \leqq R(q_i) < k. \tag{2}$$

The bulk of the time is spent in examining the inner product

$$\sigma = \sum_{j=1}^{d} a_j R(q_j) \tag{3}$$

of the case vector (1) and the trial vector

$$[a_1, a_2, \cdots, a_d] \tag{4}$$

for divisibility by k. The trial vector (4) is sparse, and in practice has less than six nonzero components. Those a's that are not zero may be replaced by their least positive remainders modulo k. The multiplication implied in (3) is accomplished instantly by replacing the case vector (1) by a "case matrix" M of k rows and d columns whose first row is (1), and whose ith row and jth column element is $iR(q_j)$ taken modulo k. Thus multiplication is accomplished by "table look-up."

Instead of storing the trial vector (4) in one or two machine words, as was done originally, each component a_j is replaced by an addition instruction with a tag of $a_j - 1$ and an address A_j of $R(q_j)$. Execution of such an instruction automatically selects from M the correct contribution to the sum and accumulates it forthwith. The final addition instruction, corresponding to the last nonzero a, is followed by a transfer command to that part of the program that tests whether σ is divisible by k. Since $\sigma < 5(k - 1)$ is of modest size, it is possible to use the following device to test divisibility by k in only 3 addition times. The early part of the memory is filled with transfer commands. The command in A, where $A < 5(k - 1)$, instructs the machine to transfer to one of two possible addresses according as A is divisible by k or not. With the quantity σ already in the accumulator the machine enters the test for divisibility by storing σ in the address of the next instruction which now reads "transfer to σ." In address σ it encounters the transfer instruction whose execution sends control to the appropriate part of the program according as k divides σ or not.

The main program was run on an IBM 7090 with seven index registers, of which six were used in the calculation of σ. More than 32000 words were used to represent the trial vectors of dimensions $\leqq 22$. Whenever the proof tree demanded the extension of the case vector beyond dimension 22, this vector was reported, the proof tree was severely pruned back to the next case vector of dimension 6 and the run was resumed.

4. Case Test. In previous papers dealing with $k < 7$, a maximal vector was obtained as an extension of a case vector the machine was unable to handle in which $R(q) = 1$ for all q's exceeding those used in the trial vectors. The machine was instructed to find the least pair $(n, n + 1)$ with $R(n) = R(n + 1) = 0$, which we shall call a "zero pair." This pair was then examined and a suitable change was made in the character of one of the factors of $n(n + 1)$. A rerun was made to search for a larger zero pair. After several such runs the desired limit was reached.

In order to speed up this process a more automatic program was written, which not only finds the first zero pair for a given vector, but also changes the case vector itself, using the following simple strategy: the largest prime factor q of the zero pair $(n, n + 1)$ is examined. If q is not on either a "fixed" or a "special" list, then $R(q)$ has been 1. The machine accordingly sets $R(q) = 2$ and puts q on the special list. If q is on the special list, then $R(q)$ has been 2, and the machine puts $R(q) = 0$ and places q on the fixed list. If q is on the fixed list, then $R(q)$ cannot be changed, and the machine selects the next largest prime factor of $n(n + 1)$ for q. When all prime factors of $n(n + 1)$ become fixed, the machine reports this impasse and stops.

This simple strategy was arrived at by studying the maximal vectors for $k < 7$ given in Table II. In some instances it was found to be a little too simple, and human intervention was required to make a change not prescribed by the strategy.

The program was tested, beginning with the simple initial vector $R(2) = 1$, $R(3) = 0$, $R(q) = 1$ for all primes $q > 3$, for all $k < 7$. The strategy worked for all $k < 6$, producing the maximal vectors given in Table II. However, in the case $k = 6$ a small amount of prompting from the authors was needed.

The maximal case vector for $k = 7$ given in Table II was obtained in this way with only two deviations from the machine strategy.

5. Case Test Program. This program is designed to evaluate $R(n)$ for a given case vector over a given interval (n_0, n_1). If a zero pair is discovered it is reported, and the automatic revision section of the program is entered. If on the other hand no zero pair is encountered in the interval, the machine stops with the remark "the limit has been reached." In particular, this happens whenever a maximal case vector and a limit $L = \Lambda(k)$ are used.

In scanning the given interval the program actually evaluates $R(n)$ only for every other n, inasmuch as it is necessary to examine $n + 1$ or $n - 1$ if and only if $R(n) = 0$. This pace is normal for the routine. After a revision, however, it is necessary to re-evaluate $R(q)$ for all multiples of q less than the current zero pair. If no multiple in this range is one of a zero pair, then the program has successfully reached the level of the current zero pair and can proceed once more at its normal pace. For $n \sim 2 \cdot 10^6$ the scanning rate is about a thousand numbers per second.

The first stage in the evaluation of $R(n)$ with respect to a given case vector consists in the complete factorization of $n = \prod_{j=1}^{t} q_j^{\alpha_j}$. This being done, it is next necessary to compute $\sum_{j=1}^{t} \alpha_j R(q_j) \pmod{k}$. Since $R(q)$ is assigned only the values 0, 1 and 2, for $j > 1$, it is possible to design a rapid look-up procedure, carried out for each factor q^α of n, consisting of three transfer commands executed consecutively.

The first of these sends control to the memory location q itself for $q < 31872$

(larger q's are handled specially). At location q a second transfer has been placed during the initial phase of the program. This transfer sends control to a list determined by $R(q)$ at a position corresponding to the multiplicity of q. Here the third transfer sends control back to the factoring section of the program, simultaneously incrementing index register 4 by the amount $\alpha R(q) \pmod k$. At the end of the factoring process the contents of index register 4 are reduced modulo k to give $R(n)$.

6. A General Inequality for $\Lambda(k)$. The case vector

$$[1, 0, 1, 1, \cdots, 1, \cdots] \tag{5}$$

is of use not only for special values of k. We use it in what follows to prove in general the

THEOREM. *If $k > 3$, and if k is odd or twice a prime of the form $4m + 3$, then $\Lambda(k) > 5^k$.*

In the proof we use the following lemmas:

LEMMA 1. *Let p be a prime $\neq 3$ and let ν be the smallest positive integer h for which $(3^h - 1)/2$ is divisible by p. Let p^r be the highest power of p dividing $(3^\nu - 1)/2$. Then p divides $(3^n - 1)/2$ if and only if ν divides n. If $n = \nu p^\beta m$, where p does not divide m, then the highest power of p dividing $(3^n - 1)/2$ is $p^{r+\beta}$.*

This is a combined statement of the familiar Laws of Apparition and Repetition of Lucas' Function $U_n = (a^n - b^n)/(a - b)$ in the special case $a = 3$, $b = 1$, [9].

LEMMA 2. *Let h be an integer >1 and let 2^{α_1}, 5^{α_2}, 7^{α_3} be the highest powers of 2, 5, and 7 dividing any of the numbers $3^n - 1$ for $n \leqq h$. Then*

$$\alpha_1 < 1.4427 \log h + 2, \tag{6}$$

$$\alpha_2 < .6214 \log h + .1387, \tag{7}$$

$$\alpha_3 < .5139 \log h + .0793. \tag{8}$$

Proof. Lemma 2 is simply the result of applying Lemma 1 to $p = 2$, 5 and 7. In fact if $p = 2$, then $\nu = 2$ and $r = 2$. Hence if

$$2^\theta \leqq h < 2^{\theta+1}$$

we may set $n = 2^\theta$ in Lemma 1 and conclude that $3^n - 1$ is divisible by a higher power of 2 than any of the numbers of the form

$$3^t - 1, \qquad t = 1(1)h$$

and this highest power of 2 is 2^{α_1}, where by Lemma 1

$$\begin{aligned} \alpha_1 &= 1 + r + \beta = 1 + 2 + \theta - 1 \\ &= 2 + \theta < 2 + \log h/\log 2 < 1.4427 \log h + 2. \end{aligned}$$

This proves (6). The inequalities (7) and (8) are established in a similar way after noting that for $p = 5$, $\nu = 4$ and $r = 1$, and that for $p = 7$, $\nu = 6$ and $r = 1$.

LEMMA 3. *Let h be an integer >1, and let 2^{α_1}, 5^{α_2}, 7^{α_3} be the highest powers of 2, 5 and 7 dividing any of the numbers $3^n + 1$ for $n \leqq h$.*

Then

$$\alpha_1 = 2,$$

$$\alpha_2 < .6214 \log h + .5694,$$

$$\alpha_3 < .5139 \log h + .4355.$$

The proof of this lemma follows also from Lemma 1 after one notices that $3^n + 1 = (3^{2n} - 1)/(3^n - 1)$.

LEMMA 4. Let $\Omega(N)$ *denote the total number of prime factors of* N *so that*

$$\Omega(p_1^{\delta_1} p_2^{\delta_2} \cdots p_t^{\delta_t}) = \delta_1 + \delta_2 + \cdots + \delta_t .$$

Then

$$\Omega(3^n - 1) \leqq 2n/3 \qquad \text{for } n > 8 \tag{9}$$

and

$$\Omega(3^n + 1) \leqq 2n/3 \qquad \text{for } n > 3. \tag{10}$$

Proof. To establish (9) suppose that it fails for some $n > 8$ and let

$$3^n - 1 = 2^{\alpha_1} 5^{\alpha_2} 7^{\alpha_3} \prod_{i>3} p_i^{\alpha_i}$$

so that

$$\Omega(3^n - 1) = (\alpha_1 + \alpha_2 + \alpha_3) + \sum_{i>3} \alpha_i = s_1 + s_2 > 2n/3.$$

From this and Lemma 2 we deduce that

$$\begin{aligned} s_2 &> (2n/3) - s_1 = (2n/3) - (\alpha_1 + \alpha_2 + \alpha_3) \\ &\geqq (2n/3) - 2.5780 \log n - 2.2180. \end{aligned} \tag{11}$$

On the other hand $\alpha_1 \geqq 1$, since $3^n - 1$ is even, $\alpha_2 \geqq 0$ and $\alpha_3 \geqq 0$.

Therefore

$$3^n - 1 \geqq 2 \prod_{i>3} p_i^{\alpha_i} \geqq 2 \cdot 11^{s_2}.$$

Hence

$$(\log 11) s_2 + \log 2 \leqq n \log 3$$

or

$$s_2 \leqq .4582n - .2890.$$

Combining this inequality with (11) we finally get

$$n < 12.365 \log n + 9.252 \tag{12}$$

which implies $n \leqq 59$.

To complete the proof it suffices to show that (9) holds for $8 < n < 60$. For this we have only to consult tables of factorization of $3^n - 1$ for $n < 60$, [8].

The values of n given in Table IV are those for which $\Omega(3^n - 1)$ exceeds all values of $\Omega(3^h - 1)$ for $8 < h < n < 60$. We give also the values of $\Omega(3^n + 1)$ and

TABLE IV

n	$\Omega(3^n - 1)$	n	$\Omega(3^n + 1)$
9	3	4	2
10	6	5	3
12	8	9	5
16	10	15	6
24	11	21	7
32	12	39	8
40	13	45	10
48	17		

the corresponding information for $3^n + 1$ to be used in connection with (10). Since (9) holds for these values of n, it holds for all $n > 8$.

To prove (10) we proceed in the same manner, this time obtaining from Lemma 3

$$n < 5.446 \log n + 16.48,$$

which implies $n \leqq 34$. An inspection of the above values of $\Omega(3^n + 1)$ shows that (10) holds for all $n > 3$. This completes the proof of Lemma 4.

Proof of Theorem. Suppose that the theorem is false. Since

$$\Lambda(4) = 1224 > 625 = 5^4,$$

$$\Lambda(5) = 7888 > 3125 = 5^5,$$

$$\Lambda(6) = 202124 > 15625 = 5^6,$$

$$\Lambda(7) = 1649375 > 78125 = 5^7$$

the theorem would have to fail for some $k > 8$. This means that every $p \neq p^*$ has two consecutive kth power residues, the first of which is $\leqq \Lambda(k)$, and hence $< 5^k$. One of these two residues is odd. Let it be denoted by ω and its companion by $\omega \pm 1$. Let us suppose that p has been chosen so that 3 is a kth power residue and that $R(q) = 1$ for all other primes $q < 5^k$. Such a p exists for k odd or twice prime of the form $4m + 3$ by [3].

Since

$$\omega \leqq \Lambda(k) < 5^k$$

and ω is an odd kth power residue, it follows that ω must be some power of 3, say 3^n, so that

$$\omega = 3^n < 5^k. \tag{13}$$

Now the kth power residue

$$\omega \pm 1 = 3^n \pm 1$$

must be such that $\Omega(3^n \pm 1)$ is a multiple of k. Since $R(q) = 1$, $(q \neq 3)$,

$$\Omega(3^n \pm 1) \geqq k. \tag{14}$$

On the other hand by (13), since $27 > 25$,

$$k > n \log 3/\log 5 > 2n/3$$

so that

$$\Omega(3^n \pm 1) > 2n/3.$$

By Lemma 4 this means that $n \leqq 8$. But no number $3^n \pm 1$ with $n \leqq 8$ has more than 7 prime factors and so (14) becomes $7 \geqq k$. This contradicts $k > 8$.

7. The Case $k = 9$. Using the same methods of proof the inequality of the theorem can be strengthened to $7 \cdot 5^{k-1}$ if one is willing to examine factors of $5^n \pm 1$. The same general method can also be used for special values of k. For instance for $k = 9$, we have examined for possible consecutiveness the 18 odd ninth power residues between 5^9 and 10^7 of primes corresponding to the case vector (5).

There is only one such pair

$$7109375 = 5^7 \cdot 7 \cdot 13, \; 7109376 = 2^8 \cdot 3 \cdot 9257.$$

With $R(9257) = 0$ the multiples of 9257 in the range 5^9 to 10^7 reveal no further pair. Hence $\Lambda(9) > 10^7$.

8. The Case $k = 8$. The first value of k not covered by the theorem is $k = 8$. However, a lower bound for $\Lambda(8)$ can be established using the case test routine. Since 2 is a quadratic residue of $p = 8m + 1$, we cannot choose $R(2) = 1$, and the case vector (5) must be modified accordingly. Starting with $R(2) = 2, R(3) = 0$ and $R(q) = 1$ for $q > 3$, the machine was able to postpone the appearance of two consecutive eighth power residues till the pair

$$(1200744 = 2^3 \cdot 3^4 \cdot 17 \cdot 109, \; 1200745 = 5 \cdot 7^2 \cdot 13^2 \cdot 29)$$

corresponding to the case vector shown in Table V. Hence $\Lambda(8) \geqq 1200744$.

TABLE V

$K = 8$	$R(3) = 0.$ $R(q) = 2$ for $q = 2$, 13, 31, 101, 113, 139, 149, 271, 317, 353, 379, 401, 443, 479, 641, 647, 673, 709, 1061, 1301, 1409, 1451, 2383, 2411, 2687, 3257, 4241, 4547, 5407, 5791, 5867, 6343, 6761, 8543, 9343, 10271, 14869, 24049. $R(q) = 1$ for all other primes < 1200744.

9. The Case $k = 10$. This is the next case not covered by the theorem. Since $p = 10m + 1$, we must have $R(5)$ even. Starting with $R(5) = 0$, $R(q) = 1$ for all $q \neq 5$, the machine arrived at the following vector:

$$R(5) = R(163) = 0,$$

$$R(q) = 2 \quad \text{for} \quad q = 47, 101, 313, 433, 593, 719, 1049, 7039,$$

$$R(q) = 1 \quad \text{for all other primes} \quad q < 22458303.$$

This vector postpones the appearance of the first pair of consecutive tenth power residues till the pair $(22458303 = 3^9 \cdot 7 \cdot 163, 22458034 = 2^6 \cdot 11 \cdot 19 \cdot 23 \cdot 73)$.

Hence $\Lambda(10) \geqq 22458303$.

Our thanks are due to the computing centers of the University of California, Berkeley, and Stanford University* for the free use of machine time for this unsponsored research.

University of San Francisco
University of California, Berkeley

1. M. DUNTON, "A bound for consecutive pairs of cubic residues." (To appear.)
2. D. H. & EMMA LEHMER, "On runs of residues," *Proc. Amer. Math. Soc.*, v. 12, 1962, p. 102–106.
3. D. H. & EMMA LEHMER & W. H. MILLS, "Pairs of consecutive power residues," *Canad. J. Math.*, v. 15, 1962, p. 172–177.
4. D. H. & EMMA LEHMER & W. H. MILLS & J. L. SELFRIDGE, "Machine proof of a theorem on cubic residues," *Math. Comp.*, v. 16, 1962, p. 407–415.
5. W. H. MILLS & R. BIERSTEDT, "On the bound for a pair of consecutive quartic residues modulo a prime p," *Proc. Amer. Math. Soc.*, v. 14, 1963, p. 628–632.
6. W. H. MILLS, "Characters with preassigned values," *Canad. J. Math.*, v. 15, 1962, p. 169–171.
7. L. E. DICKSON, "Cyclotomy and trinomial congruences," *Trans. Amer. Math. Soc.*, v. 37, 1935, p. 363–380.
8. A. J. C. CUNNINGHAM & H. J. WOODALL, *Factorisation of* $(y^n \pm 1)$, Hodgson, London, 1925, p. 10–11.
9. D. H. LEHMER, "An extended theory of Lucas' functions," *Ann. of Math.*, v. 31, 1930, p. 421–422.

* The Stanford Computation Center wishes to acknowledge assistance from the National Science Foundation under grant NSF-GP948.