ANNALS OF MATHEMATICS
Vol. 62, No. 2, September, 1955
Printed in U.S.A.

THE INTRINSIC DIVISORS OF LEHMER NUMBERS

BY MORGAN WARD

(Received March 15, 1954)

1. Introduction

A prime p is called an intrinsic divisor of the Lucas number $L_k = (\alpha^k - \beta^k)/(\alpha - \beta)$ where $\alpha + \beta$ and $\alpha\beta$ are integers, if p divides L_k but does not divide L_n for $0 < n < k$. It is well known [1], [2], [8], page 283, that if α and β are themselves integers, L_k always has an intrinsic divisor unless $\alpha = \pm 2$, $\beta = \pm 1$, $k = 6$.

The question of the existence of intrinsic divisors when α and β are real but not necessarily integers was studied some time ago in these Annals by R. D. Carmichael [3], and again quite recently by C. G. Lekkenkerker [6]. In this paper, I study the intrinsic divisors of D. H. Lehmer's generalization of the Lucas numbers [5] in which merely $(\alpha + \beta)^2$ and $\alpha\beta$ are required to be integers, again under the assumption that α and β are real. The method of attack goes back in principle to Sylvester [7], page 607, and is powerful enough to furnish a complete answer. Nothing appears to be known about the intrinsic divisors of Lucas or Lehmer numbers when α and β are complex.

Let L and M be integers, with L and $K = L - 4M$ positive and $M \neq 0$. Then the roots α and β of the polynomial

$$f(z) = z^2 - (L)^{\frac{1}{2}}z + M$$

are real. Let

$$P_n = \begin{cases} (\alpha^n - \beta^n)/(\alpha - \beta), & n \text{ odd}; \\ (\alpha^n - \beta^n)/(\alpha^2 - \beta^2), & n \text{ even}. \end{cases}$$

Then P_n is an integer. The sequence

$$(P): P_0 = 0,\ P_1 = 1,\ P_2 = 1,\ \cdots,\ P_n,\ \cdots$$

gives the Lehmer numbers associated with $f(z)$. For brevity, we call (P) and P_n "real" when α and β are real.

The subscript k of P_k is called its index; p is an intrinsic divisor of P_k if $P_k \equiv 0 \pmod p$, $P_n \not\equiv 0 \pmod p$ $0 < n < k$. (P) is called "exceptional" if it contains terms P_k of index greater than two with no intrinsic divisors; any such k is called an exceptional index. Let

$$R = \begin{cases} |4LM|, & M \text{ negative}; \\ |4KM|, & M \text{ positive}. \end{cases} \tag{1.1}$$

Then our results are as follows:

THEOREM 1.1. *A real Lehmer sequence can only be exceptional if R is less than* *sixteen. A term of a real Lehmer sequence always has an intrinsic divisor if its index is greater than eighteen.*

THEOREM 1.2. *There are only three exceptional real Lehmer sequences. The associated polynomials are* $z^2 - z - 1$, $z^2 - (5)^{\frac{1}{2}}z + 1$ *and* $z^2 - 3z + 2$. *The exceptional indices for the first two sequences are six, twelve, eighteen, and for the last sequence, six.*

The last case is the exception discovered by A. S. Bang [1]; in the first case, the Lehmer numbers are the Fibonacci numbers 0, 1, 1, 2, 3, $\cdots$ and in the second case, they are simply related to the Fibonacci numbers.

2. Elementary properties of Lehmer numbers

We collect here various properties of the Lehmer numbers given in Lehmer's Thesis [5] which are needed in what follows.

We may assume that L and M are co-prime. For if $(L, M) = D > 1$ then $L = DL'$, $M = DM'$ with $(L', M') = 1$. But if we let $\alpha = (D)^{\frac{1}{2}}\alpha'$, $\beta = (D)^{\frac{1}{2}}\beta'$ then α', β' are real when α and β are real and $(\alpha' + \beta')^2 = L'\ \alpha'\beta' = M'$ are co-prime integers. Furthermore if P'_n is the Lehmer number corresponding to α' and β', then $P_n = D^{[\frac{1}{2}(n-1)]}P'_n$ so that P_n and P'_n have the same intrinsic divisors. *We may assume that L is positive*; for if we let $\alpha = i\alpha'$, $\beta = i\beta'$ the signs of L and M are changed, and P_n is multiplied by ± 1. Since α and β are to be real, we have:

$$L > 0, \qquad K = L - 4M > 0, \qquad M \neq 0, \quad L, M \text{ co-prime.} \tag{2.1}$$

Carmichael [3] has shown by simple examples that if α and β are complex, there may be many exceptional indices.

Let n be an integer greater than two and let

$$Q_n(z, w) = \prod_{\substack{1 \leq r \leq n \\ (r,n)=1}} (z - e^{2\pi i r/n} w) \tag{2.2}$$

be the homogeneous cyclotomic polynomial of degree $\phi(n)$. We call the sequence

$$(Q)\colon Q_0 = 0,\ Q_1 = 1,\ Q_2 = 1,\ \cdots,\ Q_n = Q_n(\alpha, \beta),\ \cdots$$

the cyclotomic numbers associated with the Lehmer numbers (P). Q_n is an integer, and

$$P_n = \prod_{d|n} Q_d \tag{2.3}$$

where the product is extended over all divisors d of n. *(P) is a divisibility sequence*; that is, if n divides m, then P_n divides P_m.

The "rank" of a prime p in (P) is the least positive value k of the index n such that $P_n \equiv 0 \pmod{p}$. If p divides M, it divides no term of (P) save P_0 and we assign to it rank zero. Otherwise k exists, and divides $p - (k/p)$. The basic property of the rank of a prime may be stated as follows:

LEMMA 2.1. *Every prime number p has a rank $k \geqq 0$ in (P) such that p divides P_n if and only if k divides n.*

Consider next the ranks of powers of a prime. Clearly powers of p can only divide terms whose indices are multiples of k. Let

$$p^t \parallel P_k, \; t \geqq 1; \; P_n \not\equiv 0 \pmod{p} \; 0 < n < k. \tag{2.4}$$

That is, p^t exactly divides P_k and $P_k \div p^t$ is prime to p. Assume that $P_n \equiv 0 \pmod{p}$ and let $p^r \parallel n/k$, $r \geqq 0$.

LEMMA 2.2. *Under the hypotheses just given, p^{r+t} exactly divides P_n.*

3. The divisors of the cyclotomic numbers

A prime p which divides Q_n is called an extrinsic or intrinsic divisor according as it does or does not divide some Q_m of positive index less than n. Evidently p is an intrinsic divisor of Q_n if and only if p is an intrinsic divisor of P_n. Furthermore, if p is an extrinsic divisor of Q_n, p divides Q_d where d is a proper divisor of n. In the lemmas that follow, p is a fixed prime with positive rank k in (P), satisfying condition (2.4).

LEMMA 3.1. *Under the hypotheses just given, for every positive exponent r, p exactly divides Q_{p^rk}.*

PROOF. We make an induction on r. First, let $r = 1$, $n = pk$. Then by (2.3),

$$P_n = Q_n P_k Q', \qquad Q' = \prod Q_d \tag{3.1}$$

where the product is extended over all proper divisors d of n which are not divisors of k. If the product is empty, we take $Q' = 1$.

Then $(Q', p) = 1$. For otherwise p divides some Q_d, and hence the corresponding P_d. But then by Lemma 2.1, $k \mid d$ contrary to $d \nmid k$, $d \mid pk$, $d < pk$.

Now $p^t \parallel P_k$ and $p^{t+1} \parallel P_n$ by Lemma 2.2. Hence (3.1) implies that $p \parallel Q_n$.

Assume that the lemma is true for $n = pk, \cdots, p^{r-1}k$ and let $n = p^rk$. Then by (2.3),

$$P_n = Q_n P_k Q_{pk} Q_{p^2k} \cdots Q_{p^{r-1}k} Q', \qquad Q' = \prod Q_d$$

where the product is now extended over all divisors d of n which neither divide k nor are of the form p^sk with $1 \leqq s \leqq r$. Then $(Q', p) = 1$ as in the case $r = 1$. By Lemma 2.2, $p^{t+r} \parallel P_n$. But $p^t \parallel P_k$ and by the hypothesis of the induction, $p \parallel Q_{p^sk}$, $1 \leqq s \leqq r - 1$. Hence $p \parallel Q_n$, which completes the proof.

LEMMA 3.2. *With the previous hypotheses, let $P_n \equiv 0 \pmod{p}$ so that $n = kqp^r$ with $r \geqq 0$ and q prime to p. Then if q is greater than one, p does not divide Q_n.*

PROOF. As in the previous proof,

$$P_n = Q_n P_k Q_{pk} \cdots Q_{p^rk} Q'$$

where Q' is an integer. By Lemma 2.2, if $p^t \parallel P_k$, then $p^{r+t} \parallel P_n$ and by Lemma 3.1, $p \parallel Q_{p^sk} (s = 1, \cdots, r)$. Hence Q_n is prime to p.

The following two lemmas are easy consequences of these results.

LEMMA 3.3. *An extrinsic prime divisor of Q_n divides it to the first power only.*

LEMMA 3.4. *A sufficient condition that P_n have an intrinsic prime divisor is that $|Q_n| > n$.*

4. Inequalities for the cyclotomic numbers

We next derive some inequalities for $|Q_n|$ which enable us to use Lemma 3.4 to prove the existence of intrinsic divisors.

If $n \geqq 3$ and $\varepsilon = e^{2\pi i/n}$, then by (2.2)

$$Q_n^2 = \prod (\alpha - \varepsilon^r\beta) \prod (\alpha - \varepsilon^{-r}\beta) = \prod (\alpha^2 + \beta^2 - \alpha\beta(\varepsilon^r + \varepsilon^{-r})).$$

Here and later the products are extended over all positive integers r less than n and prime to it. Hence

$$Q_n^2 = \prod (L - 4M \cos^2 r\pi/n) = \prod (K + 4M \sin^2 r\pi/n).$$

Note also that by (2.2)

$$\prod 4 \sin^2 r\pi/n = \prod (1 - \varepsilon^r)(1 - \varepsilon^{-r}) = Q_n^2(1, 1) \geqq 1,$$

$$\prod 4 \cos^2 r\pi/n = \prod (-1 - \varepsilon^r)(-1 - \varepsilon^{-r}) = Q_n^2(-1, 1) \geqq 1.$$

Now if R is defined as in (1.1) of the introduction,

$$L - 4M \cos^2 r\pi/n > R^{\frac{1}{2}} 2 \,|\cos r\pi/n| \qquad \text{if } M < 0;$$

$$K + 4M \sin^2 r\pi/n > R^{\frac{1}{2}} 2 \,|\sin r\pi/n| \qquad \text{if } M > 0.$$

Hence in either case, we obtain the inequality

$$|Q_n| > R^{\frac{1}{4}\phi(n)}. \tag{4.1}$$

Since $R \geqq 4$, Lemma 3.4 gives us

THEOREM 4.1. *A sufficient condition that the Lehmer number of index n has an intrinsic divisor is that*

$$2^{\frac{1}{2}\phi(n)} \geqq n. \tag{4.2}$$

We next determine for what n this inequality is satisfied.

LEMMA 4.1. *If $n \geqq 2\cdot 10^9$, then*

$$\phi(n) > \frac{n}{\log n}. \tag{4.3}$$

PROOF. Since

$$\phi(n) = n \prod\nolimits_{p|n} \left(1 - \frac{1}{p}\right) \tag{4.4}$$

it suffices to show that

$$-\log \prod\nolimits_{p|n} \left(1 - \frac{1}{p}\right) < \log\log n, \qquad \text{for } n \geqq 2\cdot 10^9.$$

But by a familiar procedure (Hardy and Wright [4], Chap. 22)

$$-\log \prod\nolimits_{p|n} \left(1 - \frac{1}{p}\right) < \sum\nolimits_{p|n} \frac{1}{p} + \frac{1}{2} < \sum\nolimits_{p \leqq \log n} \frac{1}{p} + \frac{1}{\log\log n}\,\frac{1}{2}.$$

But by summation by parts and the trivial inequality $\pi(x) < 2x/\log x$,

$$\sum_{p\leq x}\frac{1}{p} < \frac{2}{\log x} + 2\log\log x - 2\log\log 2,$$

so that

$$-\log\prod_{p|n}\left(1-\frac{1}{p}\right) < 2\log\log\log n + \frac{3}{\log\log n} + \frac{1}{2} - 2\log\log 2$$
$$< \log\log n$$

since n is large.

LEMMA 4.2. *If* $1 \leqq n < 2\cdot 10^9$, *then*

$$\phi(n) > \frac{n}{6}. \tag{4.5}$$

PROOF. The product of the first nine primes is greater than $2\cdot 10^9$. Hence any number $n < 2\cdot 10^9$ has at most eight prime factors. Therefore (4.4) gives

$$\phi(n) \geqq n\prod_{2\leq p\leq 19}\left(1-\frac{1}{p}\right) = .171n > \frac{1}{6}n.$$

It follows from Lemma 4.1 that the inequality $2^{\frac{1}{2}\phi(n)} > n$ is true for large n. It also holds for $75 \leqq n < 2\cdot 10^9$ by Lemma 4.2; for in that range, $n > 12\log n/\log 2$ so that (4.5) implies that $\frac{1}{2}\phi(n)\log 2 > \log n$.

Finally, by examining the tabulated values of $\phi(n)$, the inequality $2^{\frac{1}{2}\phi(n)} \geqq n$ is found to be true for $30 < n < 75$, failing for $n = 30$ and numerous smaller indices. Hence we have proved

THEOREM 4.2. *A real Lehmer number P_n always has at least one intrinsic prime divisor provided that its index n is greater than thirty.*

5. Intrinsic divisors of Lehmer numbers of low index

It remains to discuss the Lehmer numbers of index thirty or less. The first seven cyclotomic numbers are:

$$\begin{aligned} &Q_0 = 0, \quad Q_1 = 1, \quad Q_2 = 1, \quad Q_3 = L - M, \quad Q_4 = L - 2M, \\ &Q_5 = L^2 - 3ML + 3M^2, \quad Q_6 = L - 3M. \end{aligned} \tag{5.1}$$

Hence

$$Q_8 = Q_4(Q_4 + 4M) + M^2, \qquad Q_{10} = Q_5 - 2MQ_4, \qquad Q_{12} = Q_4^2 - 3M. \tag{5.2}$$

The conditions $L, K > 0$, $M \neq 0$ and $(L, M) = 1$ easily give

LEMMA 5.1. *P_3, P_4 and P_5 always have intrinsic divisors. P_6 has an intrinsic divisor prime to L unless $L = 5$, $M = 1$, $K = 1$; $L = 1$, $M = -1$, $K = 5$;* or *$L = 9$, $M = 2$, $K = 1$.*

In the first two cases $R = 4$ and $P_6 = 8 = 4P_3$ or $2P_3$. In the third case, $R =$

8 and $P_6 = 63 = LP_3$. This is the exception $\alpha = 2$, $\beta = 1$ mentioned in the introduction.

The following table lists all indices n between 3 and 31 for which $4^{\frac{1}{2}\phi(n)}$ is less than n (so that Theorem 4.1 is inapplicable) along with the corresponding values of $\phi(n)$ and $R^{\frac{1}{2}\phi(n)}$ for $R \leqq 16$. The entry for $R^{\frac{1}{2}\phi(n)}$ is listed only if it is smaller than n; otherwise, it is starred, and has an intrinsic divisor by the inequality (4.1) and Lemma 3.4.

TABLE OF POSSIBLE EXCEPTIONAL INDICES

	$n =$	4	5	6	8	9	10	12	14	16	18	20	24	30
R	$\phi(n) =$	2	4	2	4	6	4	4	6	8	6	8	8	8
4		2	4	2	4	8	4	4	8	16	8	16	16	16
8	$R^{\frac{1}{2}\phi(n)} =$	2.8	*	2.8	8	*	8	8	*	*	*	*	*	*
12		3.5	*	3.5	*	*	*	12	*	*	*	*	*	*
16		4	*	4	*	*	*	*	*	*	*	*	*	*

Since the entries for $R = 16$ beyond $n = 6$ are all starred, Theorem 2.1 follows from Lemma 5.1 and Theorem 4.2. We also observe that if $16 > R > 4$, then 8, 10 and 12 are the only possible exceptional indices. These are disposed of by the following lemmas.

LEMMA 5.2. *If* $R = 8$ *or* 12, *then twelve is not an exceptional index.*

PROOF. Since $(L, M) = 1$ we see from the list of Q's in (5.1) that $(Q_3, M) = (Q_4, M) = (Q_6, M) = 1$. Also $Q_4 = Q_3 - M = Q_6 + M$. Hence by (5.2) $(Q_{12}, Q_6) = (Q_{12}, Q_3) = (-2M^2, Q_3) = (2, Q_3) = 1$ or 2 and $(Q_{12}, Q_4) = (-3M^2, Q_4) = (3, Q_4) = 1$ or 3.

Since $|Q_n| \geqq 8$ if neither 2 nor 3 are divisors of Q_{12}, Q_{12} has an intrinsic divisor $\geqq 5$. If either 2 or 3 are intrinsic divisors of Q_{12}, there is nothing to prove. Finally if both 2 and 3 are extrinsic divisors of Q_{12} they are the only extrinsic divisors, and by Lemma 3.3 $2 \parallel Q_{12}$, $3 \parallel Q_{12}$. Hence the quotient $Q_{12}/6$ is an integer greater than one and prime to Q_3, Q_4, Q_6. Therefore in every case Q_{12} has an intrinsic divisor.

The next lemma may be proved similarly.

LEMMA 5.3. *If* $R = 8$, *then eight and twelve are not exceptional indices.*

There remains then only the two cases when $R = 4$; namely $L = 1$, $M = -1$ and $K = 5$ or $L = 5$, $M = 1$ and $K = 1$.

In the first case, the Lehmer numbers are simply the well known Fibonacci numbers 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, $\cdots$. By direct computation, $F_6 = 2^3$, $F_{12} = 2^4 3^2$, $F_{18} = 2^3/17^2$ are the only exceptional Fibonacci numbers of index less than thirty-one.

In the second case, $P_n = F_n$ when n is even. But all possible exceptional indices are even. Hence again 6, 12 and 18 are the only exceptional indices. This argument completes the proof of Theorem 1.2 of the introduction.

In closing, note that our results immediately apply to the associated Lehmer numbers (S) defined by

$$S_n = \begin{cases} (\alpha^n + \beta^n) & n \text{ even;} \\ (\alpha^n + \beta^n)/(\alpha + \beta) & n \text{ odd.} \end{cases}$$

For $S_n = P_{2n}/P_n$.

CALIFORNIA INSTITUTE OF TECHNOLOGY

REFERENCES

[1] A. S. BANG, *Taltheoretiske Undersogelser*, Tidsskrift fur Mat. (5), 4 (1886), pp. 130–132.
[2] G. D. BIRKHOFF and H. S. VANDIVER, *On the integral divisors of $a^n - b^n$*, Ann. of Math. (2), 5 (1904), pp. 173-180.
[3] R. D. CARMICHAEL, *On the numerical factors of arithmetic forms*, Ann. of Math., 15 (1913–1914), pp. 30–70.
[4] G. H. HARDY and E. M. WRIGHT, The Theory of Numbers, Oxford, 1938.
[5] D. H. LEHMER, *An extended theory of Lucas' functions*, Ann. of Math., 31 (1930), pp. 419-448.
[6] C. G. LEKKENKERKER, *Prime factors of the elements of certain sequences of integers*, Proc. Amsterdam Akad. A 56, no. 3 (1953), pp. 265–280.
[7] J. J. SYLVESTER, Collected Mathematical Papers, 4, Cambridge University Press, 1912.
[8] K. ZSIGMONDY, *Zur theorie der Potenzreste*, Monatshefte Math. Phys., 3 (1892), pp. 265–284.