A PROPERTY OF LEHMER NUMBERS

A. SCHINZEL

Abstract. Let L, M be integers, $L > 0$, $M \neq 0$, $(L, M) = 1$ and $L \neq M, 2M, 3M, 4M$; $K = L - 4M$, $\alpha = (L^{1/2} + K^{1/2})/2$, $\beta = (L^{1/2} - K^{1/2})/2$, $P_n = (\alpha^n - \beta^n)/(\alpha^{(n,2)} - \beta^{(n,2)})$. It is proved for all positive integers k, l and m, that if $P_k | P_{lm}/P_m$, then $l \geq k/30$ and for $L > 4M$ then $l \geq k/2$.

I have proved in a previous paper [4] that if $a > b$ are coprime positive integers such that

$$\frac{a^k - b^k}{a - b} \,\Big|\, \sum_{j=0}^{n-1} c_j a^j b^{n-1-j},$$

then

$$k \leq \sum_{j=0}^{n-1} c_j.$$

It follows, hence, that if

$$\frac{a^k - b^k}{a - b} \,\Big|\, \frac{a^{lm} - b^{lm}}{a^m - b^m},$$

then $k \leq l$. The aim of this paper is to generalize the latter result in a slightly weaker form to the case, where

$$\alpha = \frac{\sqrt{L} + \sqrt{K}}{2}, \qquad \beta = \frac{\sqrt{L} - \sqrt{K}}{2} \qquad (\alpha, \beta \text{ replace } a, b), \tag{1}$$

$L > 0$, $M \neq 0$, $K = L - 4M$, and L, M are coprime integers such that α/β is not a root of unity. We shall formulate our result in terms of Lehmer numbers defined, as usual, by the formula

$$P_n = \begin{cases} \dfrac{\alpha^n - \beta^n}{\alpha - \beta}, & n \text{ odd}, \\ \dfrac{\alpha^n - \beta^n}{\alpha^2 - \beta^2}, & n \text{ even}. \end{cases} \tag{2}$$

We shall prove the following theorem.

Theorem. *Let k, l, m be positive integers and L, M integers. If*

$$L > 0, \quad M \neq 0, \quad (L, M) = 1, \quad L/M = 1, 2, 3, 4, \tag{3}$$

(1) *holds and*

$$P_k(\alpha, \beta) \mid P_{lm}(\alpha, \beta)/P_m(\alpha, \beta), \tag{4}$$

then $l \geq \frac{k}{30}$. If, in addition, $L > 4M$, then $l \geq \frac{k}{2}$.

The proof is based on nine lemmas, in which $Q_n(x, y)$ denotes the homogeneous form of a cyclotomic polynomial of order n.

Lemma 1. *If n is not of the form 2^λ or $3 \cdot 2^\lambda$, $\lambda \geq 0$, then the only factor of $Q_n(\alpha, \beta)$ that divides $nP_m(\alpha, \beta)$ for $m < n$ is the largest prime factor of n. If $n = 2^\lambda$ or $3 \cdot 2^\lambda$, $\lambda > 2$, then 2 is the only factor of $Q_n(\alpha, \beta)$ that divides $nP_m(\alpha, \beta)$ for $m < n$. If $n = 12$, $Q_{12}(\alpha, \beta)$ may have 2, 3 or 6 as factors that divide $nP_m(\alpha, \beta)$ for $m < n$.*

Proof. See [3], Theorem 3.4. □

Lemma 2. *If (1) and (2) hold and $d > 30$, then $Q_d(\alpha, \beta)$ has a prime factor not dividing d. If, in addition $L > 4M$, then the same conclusion holds for $d > 2$ except for*

$$\begin{aligned} &d = 3, \quad L = 1, \quad M = -2; \\ &d = 6, \quad L = 9, \quad M = 2; \quad L = 1, \quad M = -1 \quad \text{or} \quad L = 5, \quad M = 1; \\ &d = 12, \quad L = 1, \quad M = -1 \quad \text{or} \quad L = 5, \quad M = 1; \end{aligned} \tag{5}$$

Proof. See [1] and [2]. □

Lemma 3. *If (1) and (3) hold, then every prime factor of $Q_d(a, b)$ not dividing d is $\equiv \pm 1 \pmod{d}$.*

Proof. See [3], Theorem 3.2 and 3.3. □

Lemma 4. *If (1) and (3) hold and $d > 30$ the largest prime factor of $Q_d(\alpha, \beta)$ not dividing d exists and is at least $d - 1$. If, in addition, $L > 4M$, the same conclusion holds for $d > 2$ except for (5).*

Proof. . This follows from Lemmas 2 and 3. □

Lemma 5. *If (1) and (3) hold and k, n are positive integers, then*

$$(P_k(\alpha, \beta), P_n(\alpha, \beta)) = \left|P_{(k,n)}(\alpha, \beta)\right|. \tag{6}$$

Proof. See [3], Theorem 1.4. □

Lemma 6. *If (1) and (3) hold, k, n are positive integers, $k > 30$ and*

$$P_k(\alpha, \beta) \mid P_n(\alpha, \beta), \tag{7}$$

then, $k \mid n$. If, in addition, $L > 4M$, then the same conclusion holds for $k > 2$.

Proof. It follows from Lemma 5 and (7) that

$$|P_k(\alpha, \beta)| = \left|P_{(k,n)}(\alpha, \beta)\right|. \tag{8}$$

However,

$$P_n(\alpha, \beta) = \prod_{\substack{\delta \mid n \\ \delta > 2}} Q_\delta(\alpha, \beta), \tag{9}$$

hence, (8) gives

$$\prod_{\substack{\delta \mid n \\ \delta \nmid (k,n),\, \delta > 2}} Q_\delta(\alpha, \beta) = \pm 1,$$

which, unless $k \mid n$, gives for $k > 2$, $Q_k(\alpha, \beta) = \pm 1$. By Lemma 2 this is impossible for $k > 30$ and if $L > 4M$ for $k > 2$. Exceptions (5) are not exceptions here. □

Lemma 7. *If (1)–(4) hold, $d = (k, m) > 30$ and p is any prime factor of $Q_d(\alpha, \beta)$ not dividing d, then $\operatorname{ord}_p l > \operatorname{ord}_p k$. If $L > 4M$ the same is true for $d > 2$.*

Proof. By the identity (9), divisibility (4) takes the form

$$\prod_{\substack{\delta|k\\ \delta>2}} Q_\delta(\alpha,\beta) \Bigg| \prod_{\substack{\delta|lm\\ \delta\nmid m,\,\delta>2}} Q_\delta(\alpha,\beta),$$

which implies

$$Q_d(\alpha,\beta)\prod_{\alpha=1}^{\operatorname{ord}_p k} Q_{dp^e}(\alpha,\beta) \Bigg| \prod_{\substack{\delta|lm\\ \delta\nmid m,\,\delta>2}} Q_\delta(\alpha,\beta).$$

Hence,

$$Q_d(\alpha,\beta) \Bigg| \prod_{\substack{\delta|lm\\ \delta\nmid m,\,\delta>2,\,\delta\neq dp^e\ (1\le e\le \operatorname{ord}_p k)}} Q_\delta(\alpha,\beta).$$

By Lemma 1 if $|Q_d(\alpha,\beta)|>1$ we have either $\delta\,|\,d$, or $\delta/d=p^f$ $(f>\operatorname{ord}_p k)$. The first option is impossible, since $\delta\nmid m$ and $d\,|\,m$. The second option gives $p^f d\,|\,lm$, $p^f d\nmid m$;

$$p^f\,|\,l\frac{m}{d},\qquad p^f\nmid\frac{m}{d},$$

thus if $\operatorname{ord}_p k>0$, then $\operatorname{ord}_p m=0$ and $\operatorname{ord}_p l>\operatorname{ord}_p k$. If $\operatorname{ord}_p k=0$, then $\operatorname{ord}_p l>0$. In cases (5) the assertion is void. □

Lemma 8. *If* $L=1$, $M=-2$ *or* $L=9$, $M=2$, n *even, and* (1) *holds, then*

$$\operatorname{ord}_3 P_n(\alpha,\beta)=\operatorname{ord}_3 n.$$

Proof. This follows from the law of repetition for Lehmer numbers.

Lemma 9. *If* $n\equiv 0 \bmod 6$ *and* $L=1$, $M=-1$ *or* $L=5$, $M=1$, *and* (1) *holds, then*

$$\operatorname{ord}_2 P_n(\alpha,\beta)=\operatorname{ord}_2 n+2.$$

Proof. For $n\equiv 0 \bmod 6$ the sequences $P_n(\alpha,\beta)$ corresponding to $L=1$, $M=-1$ and $L=5$, $M=1$ coincide and the lemma follows from the law of repetition for Lehmer numbers.

Proof of the Theorem. Let $d=(k,m)$. By Lemma 6 we have $k\,|\,lm$, hence $\frac{k}{d}\,|\,l$. Also, by Lemmas 2 and 7, if $d>30$ or $L>4M$ and $d>2$ and exceptions (5) are excluded, a prime factor of $Q_d(\alpha,\beta)$ not dividing d exists and divides l in a higher power than k. Hence by Lemma 4,

$$l\ge p\frac{k}{d}\ge (d-1)\frac{k}{d}>\frac{k}{2}.$$

Now consider the cases (5).

If $d=3$, $L=1$, $M=-2$, then by Lemma 6

$$\frac{k}{3}\,\Big|\,l. \tag{10}$$

On the other hand, by Lemma 8

$$\operatorname{ord}_3 P_k(\alpha,\beta)=\operatorname{ord}_3 k,$$
$$\operatorname{ord}_3 P_{lm}(\alpha,\beta)/P_m(\alpha,\beta)=\operatorname{ord}_3 l,$$

hence, by (4), $\operatorname{ord}_3 k\le\operatorname{ord}_3 l$ and, by (10), $k\,|\,l$.

If $d = 6$, $L = 9$, $M = 2$, then by Lemma 6

$$\frac{k}{6} \Big| l. \tag{11}$$

On the other hand, by Lemma 8, as above $\text{ord}_3 k \le \text{ord}_3 l$ and, by (11)

$$\frac{k}{2} \Big| l.$$

If $d = 6$ or 12, $L = 1$, $M = -1$ or $L = 5$, $M = 1$, then by Lemma 6

$$\frac{k}{d} \Big| l. \tag{12}$$

On the other hand, by Lemma 9

$$\text{ord}_2 P_k(\alpha, \beta) = \text{ord}_2 k + 2,$$
$$\text{ord}_2 P_{lm}(\alpha, \beta)/P_m(\alpha, \beta) = \text{ord}_2 l,$$

hence, by (4), $\text{ord}_2 k + 2 \le \text{ord}_2 l$ and, by (12),

$$\frac{4}{3}k \Big| l.$$

References

[1] Yu. Bilu, G. Hanrot, and P. M. Voutier, *Existence of primitive divisors of Lucas and Lehmer numbers, with an appendix by M. Mignotte*, J. Reine Angew. Math., **539** (2001), 75–122.

[2] L. K. Durst, *Exceptional real Lehmer sequences*, Pac. J. Math., **9** (1959), 437–441.

[3] D. H. Lehmer, *An extended theory of Lucas' functions*, Ann. of Math., **31.2** (1930), 419–448.

[4] A. Schinzel, *On divisibility by* $\frac{a^k - b^k}{a - b}$, The Fibonacci Quarterly, **51.1** (2013), 72–77.

MSC2010: 11B39

Institute of Mathematics, Polish Academy of Sciences, Śniadeckich 8, 00-956 Warsaw, Poland
E-mail address: schinzel@impan.pl