A PROPERTY OF LEHMER NUMBERS

A. SCHINZEL

Abstract. Let $L, M$ be integers, $L > 0$, $M \neq 0$, $(L, M) = 1$ and $L \neq 1, M, 2M, 3M, 4M$; $K = L - 4M$, $\alpha = (L^{1/2} + K^{1/2})/2$, $\beta = (L^{1/2} - K^{1/2})/2$, $P_n = (\alpha^n - \beta^n)/(\alpha^{(n,2)} - \beta^{(n,2)})$. 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
\[
\frac{a^k - b^k}{a - b} \mid \sum_{j=0}^{n-1} c_j a^j b^{n-1-j},
\]
then
\[
k \leq \sum_{j=0}^{n-1} c_j.
\]

It follows, hence, that if
\[
\frac{a^k - b^k}{a - b} \mid \frac{a^{lm} - b^{lm}}{a^m - b^m},
\]
then $k \leq l$. The aim of this paper is to generalize the latter result in a slightly weaker form to the case, where
\[
\alpha = \frac{\sqrt{L} + \sqrt{K}}{2}, \quad \beta = \frac{\sqrt{L} - \sqrt{K}}{2} \quad (\alpha, \beta \text{ replace } a, b), \quad (1)
\]
$L > 0$, $M \neq 0$, $K = L - 4M$, and $L, M$ are coprime integers such that $\alpha/\beta$ is not a root of unity. We shall formulate our result in terms of Lehmer numbers defined, as usual, by the formula
\[
P_n = \begin{cases} 
\frac{\alpha^n - \beta^n}{\alpha^n - \beta^n}, & n \text{ odd}, \\
\frac{\alpha^n - \beta^n}{\alpha^2 - \beta^2}, & n \text{ even}.
\end{cases} \quad (2)
\]

We shall prove the following theorem.

Theorem. Let $k, l, m$ be positive integers and $L, M$ integers. If
\[
L > 0, \quad M \neq 0, \quad (L, M) = 1, \quad L/M = 1, 2, 3, 4, \quad (3)
\]
(1) holds and
\[
P_k(\alpha, \beta) \mid P_{lm}(\alpha, \beta)/P_m(\alpha, \beta), \quad (4)
\]
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 $n$. 

MAY 2013 119
Lemma 1. If \( n \) is not of the form \( 2^\lambda \) 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

\[
\begin{align*}
d &= 3, & L &= 1, & M &= -2; \\
d &= 6, & L &= 9, & M &= 2; & L &= 1, & M &= -1 \text{ or } L = 5, & M &= 1; \\
d &= 12, & L &= 1, & M &= -1 \text{ or } L = 5, & M &= 1;
\end{align*}
\]

Proof. See [1] and [2].

Lemma 3. If (1) and (3) hold, then every prime factor of \( Q_d(\alpha, \beta) \) 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

\[
(P_k(\alpha, \beta), P_n(\alpha, \beta)) = |P_{(k,n)}(\alpha, \beta)|.
\]

Proof. See [3], Theorem 1.4.

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

\[
P_k(\alpha, \beta) \mid P_n(\alpha, \beta),
\]

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

\[
|P_k(\alpha, \beta)| = |P_{(k,n)}(\alpha, \beta)|.
\]

However,

\[
P_n(\alpha, \beta) = \prod_{\delta \mid n} Q_\delta(\alpha, \beta),
\]

hence, (8) gives

\[
\prod_{\delta \mid n} Q_\delta(\alpha, \beta) = \pm 1,
\]

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 \( \text{ord}_p l > \text{ord}_p k \). If \( L > 4M \) the same is true for \( d > 2 \).
A PROPERTY OF LEHMER NUMBERS

Proof. By the identity (9), divisibility (4) takes the form
\[
\prod_{\delta \mid k, \delta > 2} Q_\delta(\alpha, \beta) \mid \prod_{\delta \mid lm, \delta > 2} Q_\delta(\alpha, \beta),
\]
which implies
\[
Q_d(\alpha, \beta) \prod_{\alpha=1}^{\text{ord}_p k} Q_{d^e}(\alpha, \beta) \mid \prod_{\delta \mid lm, \delta > 2} Q_\delta(\alpha, \beta).
\]
Hence,
\[
Q_d(\alpha, \beta) \prod_{\delta \mid lm, \delta > 2, \delta \neq d^e (1 \leq e \leq \text{ord}_p k)} Q_\delta(\alpha, \beta).
\]
By Lemma 1 if \(|Q_d(\alpha, \beta)| > 1\) we have either \(\delta \mid d\), or \(\delta/d = p^f (f > \text{ord}_p k)\). The first option is impossible, since \(\delta \nmid m\) and \(d \mid m\). The second option gives \(p^f d \mid lm\), \(p^f d \nmid m\); \(p^f \mid l m\), \(p^f \nmid m\). Thus if \(\text{ord}_p k > 0\), then \(\text{ord}_p m = 0\) and \(\text{ord}_p l > \text{ord}_p k\). If \(\text{ord}_p k = 0\), then \(\text{ord}_p l > 0\). 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
\[
\text{ord}_3 P_n(\alpha, \beta) = \text{ord}_3 n.
\]
Proof. This follows from the law of repetition for Lehmer numbers.

Lemma 9. If \(n \equiv 0 \mod 6\) and \(L = 1, M = -1\) or \(L = 5, M = 1\), and (1) holds, then
\[
\text{ord}_2 P_n(\alpha, \beta) = \text{ord}_2 n + 2.
\]
Proof. For \(n \equiv 0 \mod 6\) 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 \(k \mid lm\), hence \(\frac{k}{d} \mid l\). 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,
\[
l \geq p^k_d \geq (d-1) \frac{k}{d} > \frac{k}{2}.
\]
Now consider the cases (5).

If \(d = 3, L = 1, M = -2\), then by Lemma 6
\[
\frac{k}{3} \mid l.
\]
On the other hand, by Lemma 8
\[
\text{ord}_3 P_k(\alpha, \beta) = \text{ord}_3 k,
\]
\[
\text{ord}_3 P_{lm}(\alpha, \beta)/P_m(\alpha, \beta) = \text{ord}_3 l,
\]
hence, by (4), \(\text{ord}_3 k \leq \text{ord}_3 l\) and, by (10), \(k \mid l\).
THE FIBONACCI QUARTERLY

If \( d = 6, L = 9, M = 2 \), then by Lemma 6
\[
\frac{k}{6} \mid l. \tag{11}
\]
On the other hand, by Lemma 8, as above \( \text{ord}_3 k \leq \text{ord}_3 l \) and, by (11)
\[
\frac{k}{2} \mid l.
\]
If \( d = 6 \) or \( 12, L = 1, M = -1 \) or \( L = 5, M = 1 \), then by Lemma 6
\[
\frac{k}{d} \mid l. \tag{12}
\]
On the other hand, by Lemma 9
\[
\text{ord}_2 P_k(\alpha, \beta) = \text{ord}_2 k + 2,
\]
\[
\text{ord}_2 P_m(\alpha, \beta) / P_m(\alpha, \beta) = \text{ord}_2 l,
\]
hence, by (4), \( \text{ord}_2 k + 2 \leq \text{ord}_2 l \) and, by (12),
\[
\frac{4}{3} \frac{k}{3} \mid l.
\]

REFERENCES


MSC2010: 11B39