ARKIV FÖR MATEMATIK Band 4 nr 33

Communicated 11 October 1961 by T. NAGELL

The intrinsic divisors of Lehmer numbers in the case of negative discriminant

By ANDRZEJ SCHINZEL

A prime p is called an intrinsic divisor of the Lehmer number

$$P_n=\begin{cases}(\alpha^n-\beta^n)/(\alpha-\beta), & n \text{ odd},\\ (\alpha^n-\beta^n)/(\alpha^2-\beta^2), & n \text{ even},\end{cases} \tag{1}$$

where $(\alpha+\beta)^2$ and $\alpha\beta$ are integers, if p divides P_n but does not divide P_k for $0<k<n$ (cf. [10]). M. Ward [10] and L. K. Durst [4] proved that if α, β are real $((\alpha+\beta)^2, \alpha\beta)=1$ and $n \neq 6$, 12 then P_n has an intrinsic divisor. According to [10] nothing appears to be known about the intrinsic divisors of Lehmer numbers when α and β are complex, except that there may be many indices n such that P_n has no intrinsic divisor.

The aim of this paper is to prove the following

Theorem. *If α and β are complex and β/α is not a root of unity, then, for $n>n_0(\alpha,\beta)$, P_n has an intrinsic divisor. Number $n_0(\alpha,\beta)$ can be effectively computed.*

This theorem is an easy consequence of some deep theorem of Gelfond ([5] p. 174), which we quote below with small changes in the notation.

The inequality

$$|x_1 \log a + x_2 \log b| < e^{-\log^{2+\eta} x}, \quad |x_1|+|x_2|=x>0,$$

where a and b are algebraic numbers, $\log a/\log b$ is irrational, $\eta>0$ is an arbitrary fixed number, does not have a solution in rational integers x_1, x_2 with

$$x>x_0(a, b, \log a/\log b, \eta),$$

where x_0 is an effectively computable constant.

Lemma. *If α and β are complex and β/α is not a root of unity, then for every $\varepsilon>0$ and $n>N(\alpha,\beta,\varepsilon)$*

$$|P_n|>|\alpha|^{n-\log^{2+\varepsilon} n}, \tag{2}$$

$$|Q_n|=\Big|\prod_{\substack{1\le r\le n\\ (r,n)=1}}(\alpha-e^{2\pi i r/n}\beta)\Big|>|\alpha|^{\varphi(n)-2^{\nu(n)}\log^{2+\varepsilon} n}, \tag{3}$$

where $\varphi(n)$ denotes the Euler function, $\nu(n)$ the number of prime factors of n. $N(\alpha,\beta,\varepsilon)$ can be effectively computed.

Proof. Let us put in the theorem quoted above $a=\beta/\alpha$, $b=1$, $\log b=2\pi i$.

Since β/α is not a root of unity all the assumptions are fulfilled and for rational integers x_1, x_2 where $x_1 > x_0(\beta/\alpha, 1, (\log \beta/\alpha)/2\pi i, \eta) > 0$ we get

$$|x_1 \log \frac{\beta}{\alpha} + x_2 \cdot 2\pi i| \geqslant \exp(-\log^{2+\eta} c x_1), \tag{4}$$

where

$$c = \frac{|\log \beta/\alpha|}{2\pi} + 2.$$

Now $|\varphi - 2\pi k| \geqslant d$ (for all integral k) implies as can be easily seen

$$|\cos \varphi + i \sin \varphi - 1| \geqslant \tfrac{1}{2} d \quad (\varphi \text{ real}, \ 3 \geqslant d \geqslant 0).$$

Inequality (4) gives therefore for positive $x_1 > x_0$

$$\left| \left(\frac{\beta}{\alpha}\right)^{x_1} - 1 \right| \geqslant \tfrac{1}{2} \exp(-\log^{2+\eta} c x_1). \tag{5}$$

On the other hand, by (1)

$$|P_n| \geqslant \frac{|\alpha^n - \beta^n|}{|\alpha^2 - \beta^2|} = \frac{|\alpha|^n}{|\alpha^2 - \beta^2|} \left| \left(\frac{\beta}{\alpha}\right)^n - 1 \right|. \tag{6}$$

By a suitable choice of η which can be done in a completely effective manner we get (2) from (5) and (6) for $n > N_0(\alpha, \beta, \varepsilon)$. Since $(\alpha - \beta)^2 = (\alpha + \beta)^2 - 4\alpha\beta$ is an integer $\neq 0$, we have also

$$|P_n| \leqslant \frac{|\alpha^n - \beta^n|}{|\alpha - \beta|} \leqslant \frac{2|\alpha|^n}{|\alpha - \beta|} \leqslant 2|\alpha|^n. \tag{7}$$

Now since $Q_n = \prod_{d/n} P_d^{\mu(n/d)}$, it follows from (2) and (7), that

$$|Q_n| > \prod_{\substack{d/n \\ \mu(n/d)=1,\ d>N_0}} |\alpha|^{d - \log^{2+\varepsilon} d} \Big/ \prod_{\substack{d/n \\ \mu(n/d)=-1}} 2|\alpha|^d.$$

Since β/α is not a root of unity, it follows by enumeration of cases that $\alpha\beta \neq 1$, hence $|\alpha| \geqslant \sqrt{2}$. We then get

$$\frac{\log |Q_n|}{\log |\alpha|} > \sum_{d/n} \mu\left(\frac{n}{d}\right) d - \sum_{d \leq N_0} d - \sum_{\substack{d/n \\ \mu(n/d)=-1}} \log^{2+\varepsilon} d - 2 \sum_{\substack{d/n \\ \mu(n/d)=-1}} 1$$

$$\geqslant \varphi(n) - \frac{N_0(N_0+1)}{2} - 2^{\nu(n)-1} \log^{2+\varepsilon} n - \nu(n).$$

Taking $N > N_0$ so large that $\log^2 N > [N_0(N_0+1)/2] + 1$ we get for $n > N = N(\alpha, \beta, \varepsilon)$

$$\frac{\log |Q_n|}{\log |\alpha|} > \varphi(n) - 2^{\nu(n)} \log^{2+\varepsilon} n$$

hence inequality (3) holds.

Proof of the theorem. As can be easily seen (cf. [4a]) the assumption $((\alpha+\beta)^2, \alpha\beta)=1$ leads to no loss of generality. Under this assumption a sufficient condition that $P_n\,(n\neq 6)$ have an intrinsic divisor is that $|Q_n|>n$. This was proved by Ward ([10] Lemma 3.4) in connection with real α, β but his proof applies to our case also. The necessary condition $n\neq 6$ was pointed out by Durst [4].

In view of (3) which we apply for $\varepsilon=1$, and since $|\alpha|\geqslant\sqrt{2}$ it remains to find an $n_0>N(\alpha, \beta, 1)$ such that for $n>n_0$

$$\varphi(n)-2^{\nu(n)}\log^3 n>\frac{2\log n}{\log 2}.$$

Now, $\varphi(n)>n/\log n$ for $n>2\cdot 10^3$ ([10] Lemma 4.1), $2^{\nu(n)}<2\sqrt{n}$ (obviously) and the inequality

$$\frac{n}{\log n}-2\sqrt{n}\log^3 n>\frac{2\log n}{\log 2}$$

holds certainly for $n>10^{20}$. Taking $n_0=\max\,(N, 10^{20})$ we complete the proof.

An open and interesting question is whether the number $n_0(\alpha, \beta)$ which occurs in the theorem can be taken independent of α, β provided $((\alpha+\beta)^2, \alpha\beta)=1$.

By the way of example let us take a sequence P_n for $\alpha=(1+\sqrt{-7})/2$, $\beta=(1-\sqrt{-7})/2$. This sequence was considered by several authors, inter alia by T. Nagell [6], [7], J. Browkin, A. Schinzel [1], W. Sierpiński [8], T. Skolem, S. Chowla, M. Dunton, D. J. Lewis [3], [9], P. Chowla [2] (who considered P_{2n}/P_n), often in connection with the diophantine equation $x^2+7=2^n$. Principal results were as follows:

1. The equation $P_n=\pm 1$ has exactly five solutions $n=1, 2, 3, 5, 13$ (first proved by Nagell [6], also [1], [3], [7], [9]),

2. The equation $P_n=c$ has at most three solutions ([9]),

3. The equation $P_{2n}/P_n=P_{2^g+1}/P_{2^g}$ has the only solution $n=2^g$, the equation $P_{2n}/P_n=c$ has at most two solutions,

and the question was left open ([9] p. 668) how to determine a number $n_0(c)$ such that $P_n\neq c$ for $n>n_0(c)$.

It follows from the theorem proved in this paper that for $c\neq\pm P_i$ $(i=1, 2, \ldots, n_0(\alpha, \beta))$ the equation $P_n=\pm c$ has at most one solution, also if $c\neq\pm P_{2i}/P_i$ $(i=1, 2, \ldots, n_0(\alpha, \beta))$ the equation $P_{2n}/P_n=\pm c$ has at most one solution. Lemma 1 in which $N(\alpha, \beta)$ is effectively computable gives an implicit answer to the question mentioned above. However an explicit answer can be obtained directly from statements $1-2$ and from known divisibility properties of Lehmer numbers (cf. [4] § 2). In fact, suppose that $P_n=c$. For each $\delta|n$ we must have $P_\delta|c$, in particular for each prime $q|n$, $P_q|c$. Thus either $P_q=\pm 1$ or P_q is divisible by some prime $p|c$. In the first case $q=2, 3, 5$ or 13 by 1, in the second by the so called law of apparition for Lehmer numbers ([2] Theorems 2.0 and 2.1)

$$q\,|\,p-\left(\frac{-7}{p}\right),$$

hence $q\leqslant p+1\leqslant|c|+1$. Thus

$$\text{all prime factors of } n \text{ are } \leqslant|c|+12. \tag{8}$$

On the other hand by 2, the equation $p_\delta = d$ has for each $d|c$ at most three solutions. This gives the condition

$$d(n) \leqslant 6\, d(|c|), \tag{9}$$

where $d(k)$ denotes as usual, the number of positive divisors of k.

It follows from (8) and (9) that if $n > (|c| + 12)^{6d(|c|)}$, then $P_n \neq c$, which is just an answer to the question posed.

Note added in proof. There is some discordance in definitions of intrinsic divisors. According to D. H. Lehmer, a prime p is called an intrinsic divisor of P_n if p divides P_n but does not divide either $(\alpha-\beta)^2$ $(\alpha+\beta)^2$ or P_k for $0 < k < n$. It can be easily seen that the theorem proved in the paper holds also for intrinsic divisors defined in this manner.

REFERENCES

1. Browkin, J., Schinzel, A., Sur les nombres de Mersenne qui sont triangulaires. C. R. Paris *242*, 1780–81 (1956).
2. Chowla, P., A class of Diophantine equations. Proc. Nat. Acad. Sci., U.S.A. *45*, 569–570 (1959).
3. Chowla, S., Dunton, M., Lewis, D. J., All integral solutions of $2^n - 7 = x^2$ are given by $n = 3$, 4, 5, 7, 15. Det Kongl. Norske Vidensk. Selsk. Forhandl. *B 33*, nr. 9 (1960).
4. Durst, L. K., Exceptional real Lehmer sequences. Pacific Journal of Math. *9*, 437–441 (1959).

4 a ——, Exceptional real Lucas sequences, Pacific Journal of Math. *11*, 489–494 (1961).

5. Gelfond, A. O., Transcendental and Algebraic Numbers. New York, 1960.
6. Nagell, T., Løste oppgaver. Norsk Matematisk Tidsskrift *30*, 62–64 (1948).
7. ——, The Diophantine equation $x^2 + 7 = 2^n$. Arkiv för Matematik *4*, 182–185 (1961).
8. Sierpiński, W., Sur deux suites recurrentes. Matematiche Catania *12*, 23–30 (1957).
9. Skolem, T., Chowla, S., Lewis, D. J., The Diophantine equation $2^{n+2} - 7 = x^2$ and related problems. Proc. Amer. Math. Soc. *10*, 663–669 (1959).
10. Ward, M., The intrinsic divisors of Lehmer numbers. Annals of Math. (2) *62*, 230–236 (1955).

Tryckt den 24 januari 1962

Uppsala 1962. Almqvist & Wiksells Boktryckeri AB