ON A PROBLEM OF M. WARD

R. R. LAXTON
University of Nottingham, Nottingham, England

1. INTRODUCTION

In [3] M. Ward showed that a general non-degenerate integral linear recurrence of order two has infinitely many distinct prime divisors. He conjectured that the result was true for linear recurrences of higher order (again excluding certain degenerate ones) and, indeed, confirmed this in [4] for the case of cubic recurrences. Here we prove Ward's conjecture; the method is straightforward and uses the most elementary form of p-adic analysis. We end by discussing the limitations of the method together with the problems it raises and posing further questions concerning divisors of recurrences (especially in connection with the work of K. Mahler).

2. STATEMENT OF THE PROBLEM

2.1. Let the polynomial $f(x) = x^m - a_{m-1}x^{m-1} - \cdots - a_1x - a_0 \in \mathbb{Z}[x]$, $m > 1$, have no root nor ratio of distinct roots a root of unity. Say

$$f(x) = \prod_{i=1}^{m} (x - \theta_i) ,$$

where the θ_i are algebraic integers. Put $\mathbb{K} = \mathbb{Q}(\theta_1, \cdots, \theta_m)$; it is a normal extension of the rational field $\mathbb{Q}$.

$W = \{w_0, w_1, \cdots, w_n, \cdots\}$ is a (integral) linear recurrence with companion polynomial $f(x)$ if given $w_0, w_1, \cdots, w_{m-1} \in \mathbb{Z}$, not all zero, we have

$$w_{n+m} = a_{m-1}w_{n+m-1} + \cdots + a_1w_{n+1} + a_0w_n ,$$

for all non-negative integers n. Thus all the terms of W are rational integers.

2.2. We can assume that $a_0 \neq 0$ since otherwise we would have a linear recurrence of degree less than m.

All the roots $\theta_1, \cdots, \theta_m$ are distinct, so we may write

$$Dw_n = A_1\theta_1^n + \cdots + A_m\theta_m^n \tag{2.1}$$

for all n, where the A_i are algebraic integers in $\mathbb{K}$ and the rational integer D is the discriminant of $f(x)$.

If at most one of the A_i of (2.1) is not zero, then we have a degenerate recurrence and this we exclude. Hence we may assume that $A_1A_2 \cdots A_m \neq 0$ and $m \geq 2$ since otherwise we would use (2.1) but with the zero A_i's deleted.

To make the exposition clear, we shall assume that $f(x)$ splits in $\mathbf{Z}[x]$, i.e., that $\theta_1, \cdots, \theta_m$ are rational integers. The following proof remains valid in general (with prime ideals replacing rational primes, etc.) apart from one step and this we shall deal with at the end of the present proof.

2.3. An integer n is a divisor of W if n divides some term w_m of W. We shall be concerned with prime divisors of W. If a prime p divides all the roots $\theta_1, \cdots, \theta_m$ then p divides all the terms w_t of W with $t \geq m$; these divisors (which are called null-divisors) are of no interest to us and we eliminate them. Let $u = \text{g.c.d.}\ (\theta_1, \cdots, \theta_m)$ and rewrite (2.1) as

$$
\begin{aligned}
Dw_n &= u^n\left(A_1\left(\frac{\theta_1}{u}\right)^n + \cdots + A_m\left(\frac{\theta_m}{u}\right)^n\right) \\
&= u^n\left(A_1\delta_1^n + \cdots + A_m\delta_m^n\right) \quad ,
\end{aligned} \tag{2.2}
$$

with $\delta_i = \theta_i/u$ for all $i = 1, \cdots, m$. It follows that given any prime p, there is at least one δ_i which is not divisible by p. This fact we will need in the subsequent proof.

2.4. From now on we will assume that the recurrence W given by (2.1) has only a finite number of prime divisors. It follows from (2.2) that there are only a finite number of primes, say $p_1, \cdots, p_t$, which are prime divisors of the integers $U_n = A_1\delta_1^n + \cdots + A_m\delta_m^n$ for all $n = 0, 1, 2, \cdots$. Essentially we prove that this assumption implies that the terms U_n assume the same integer value for infinitely many distinct values of n.

3. THE ANALYSIS

3.1. Let $p = p_i$ be one of the primes $p_1, \cdots, p_t$ which divide some U_n. From the construction in 2.3, we know that some δ_i is not divisible by p — say $\delta_1, \cdots, \delta_d$ ($d = d(i) \geq 1$) are p-adic units and $\delta_{d+1}, \cdots, \delta_m$ are divisible by p.

For the moment, we will assume that

$$
A_1\delta_1^n + \cdots + A_d\delta_d^n = 0 \tag{3.1}
$$

for only finitely many $n \in \mathbf{Z}$, $\quad n > 0$.

Let $k = k(i)$ be such that $A_1\delta_1^k + \cdots + A_d\delta_d^k \neq 0$. Say $A_1\delta_1^k + \cdots + A_d\delta_d^k \equiv 0 \pmod{p^s}$ but $A_1\delta_1^k + \cdots + A_d\delta_d^k \not\equiv 0 \pmod{p^{s+1}}$ for some integer $s = s(i) \geq 0$. For each $j = 1, \cdots, d$, there exists a positive integer b_j such that

$$
\delta_j^{b_j} \equiv 1 \pmod{p^{s+1}} .
$$

Now put $b = b(i) = b_1b_2 \cdots b_d$. Then for each $r \in \mathbf{Z}$ such that $v = k + rb > s$, the rational integer

$$U_v = A_1\delta_1^v + \cdots + A_m\delta_m^v \equiv A_1\delta_1^v + \cdots + A_d\delta_d^v$$
$$\equiv A_1\delta_1^k + \cdots + A_d\delta_d^k \pmod{p^{s+1}}.$$

Thus for all $v = k + rb > s$, the terms U_v are exactly divisible by p^s.

3.2. Now repeat the argument of 3.1 for each of the primes $p_1, \cdots, p_t$. It is clear that provided the assumption (3.1) holds for each of these primes, the value selected for $k = k(i)$ can be chosen to be the same for all $p_1, \cdots, p_t$. Assuming then that (3.1) holds for each p_i, $i = 1, \cdots, t$, we have constructed a subsequence $U_{v(i)}$ of $\{U_n,\ n = 0, 1, \cdots\}$ for all $r \in \mathbf{Z}$ with $v(i) = k + rb(i) > s(i)$, all of whose terms are exactly divisible by $p^{s(i)}$.

Therefore for all $r \in \mathbf{Z}$ such that $v = k + rb(1)b(2)\cdots b(t) > \max(s(1), \cdots, s(t))$, the infinite subsequence $\{U_v\}$ of $\{U_n\}$ takes on the form $\pm N$ for some fixed integer N (since the primes $p_1, \cdots, p_t$ are the only prime divisors of terms of this sequence $\{U_n\}$ of rational integers).

3.3. Now both the derivation in 3.2 and the denial of assumption (3.1) for some prime among $p_1, \cdots, p_t$ give rise to statements of the form: "$A_1\delta_1^n + \cdots + A_f\delta_f^n$ takes the same value for infinitely many $n \in Z$, $n \geq 0$." Here A_i and δ_i are non-zero algebraic integers (actually we have assumed they are rational; see 2.2) and $f \geq 2$ ($f = m \geq 2$ for the derivation in 3.2 and for (3.1) to be false we must have $f = d(i) \geq 2$).

By p-adic methods (see for example K. Mahler's article [1]) we can conclude from this that some ratio δ_i/δ_j, $i \neq j$, is a root of unity and hence $\theta_i/\theta_j = u\delta_i/u\delta_j$ is a root of unity. This contradicts our initial hypothesis and so the assumption that the recurrence W has only finitely many prime divisors is false.

4. REMARK ON THE GENERALIZATION OF THE PROOF

We need consider the case when $f(x)$ does not split in $\mathbf{Z}[x]$ and so $\theta_1, \cdots, \theta_m$ are not rational integers but only algebraic integers. As we remarked in 2.2, we use prime ideals $\underline{p}$ of the normal extension $\mathbf{K}$ instead of rational primes p and $\underline{p}$-adic analysis instead of p-adic analysis. This part of the generalization causes us no trouble but there is a slight difficulty in getting rid of the null-divisors of W in 2.3 and forming Eq. (2.2). There we put $u = \text{g.c.d.}\ (\theta_1, \cdots, \theta_m)$ and subsequently considered the sequence $U_n = A_1\delta_1^n + \cdots + A_m\delta_m^n$ of rational integers — and the fact that the U_n are rational integers is important in Sec. 3.2 where we used the fact that the only units in the rationals are ± 1 (and thereby deducing that we obtained an infinite subsequence $\{U_v\}$ of $\{U_n\}$ taking the values N for some fixed $N \in \mathbf{Z}$). To overcome this we let $q_1, \cdots, q_s$ be the set (possibly empty) of all rational primes dividing g.c.d. $(a_0, \cdots, a_{m-1})$, the coefficients of $f(x)$. In the normal extension $\mathbf{K} = \mathbf{Q}(\theta_1, \cdots, \theta_m)$ let the ideal (q_i) have prime ideal decomposition

$$(q_i) = (\underline{q}_{i(1)} \cdots \underline{q}_{i(r)})^{\alpha_i}, \qquad \alpha_i \in \mathbf{Z},\ \alpha_i > 0.$$

Now each prime ideal $\underline{q}_{i(k)}$ contains all $\theta_1, \cdots, \theta_m$; let $\beta_{i(k)} > 1$ be the highest power of $\underline{q}_{i(k)}$ dividing all $\theta_1, \cdots, \theta_m$. Since $\mathbf{K}$ is normal we have

$$\beta_{i(1)} = \beta_{i(2)} = \cdots = \beta_{i(r)} = \beta_i ,$$

say. We do this for all $i = 1, \cdots, s$. Put $\alpha = \alpha_1\alpha_2 \cdots \alpha_s$ and then

$$\prod_{i,k}\left(\frac{\beta_i}{\underline{q}_{i(k)}}\right)^{\alpha} = (u) ,$$

where u is a rational integer.

Now instead of considering all terms w_n of W we consider only the subsequence $\{w_{\alpha n}\}$ and (2.2) then becomes

$$Dw_{\alpha n} = A_1\theta_1^{\alpha n} + \cdots + A_m\theta_m^{\alpha n} = u^n(A_1\delta_1^n + \cdots + A_m\delta_m^n) ,$$

with $\delta_i = \theta_i^{\alpha}/u$ for all $i = 1, \cdots, m$. Here $\{A_1\delta_1^n + \cdots + A_m\delta_m^n\}$ is a sequence of rational integer terms and for any prime $\underline{p}$ at least one δ_i is a $\underline{p}$-adic integer. The analysis can now proceed as previously.

5. PROBLEMS CONCERNING FURTHER GENERALIZATIONS

5.1. One would suppose that the result established here can be generalized to arbitrary linear recurrences, not just those W all of whose terms are integers. However, our method of proof breaks down in this general situation since in Sec. 3.2, we needed the fact that there are only a finite number of units in $\mathbf{Z}$

5.2. In [2], K. Mahler has shown (using the p-adic generalization of Roth's Theorem) that in a non-degenerate linear recurrence of order two (with c.p. $x^2 - Px + Q$, $4p > Q^2$ and $Q \geq 2$) every infinite subsequence has an infinite number of prime divisors. Again one would suppose that this is true for linear recurrences of higher order.

5.3. Let $f(x) = x^2 - Px + Q \in \mathbf{Z}[x]$, $Q \neq 0$, and $W = \{\cdots, w_0, w_1, \cdots, w_n, \cdots\}$ $w_0, w_1 \in \mathbf{Z}$ be a linear recurrence satisfying $w_{n+2} = Pw_{n+1} - Qw_n$, for all $n \in \mathbf{Z}$ (we are allowing the recurrence to go in both directions so that now not all terms are integers). Then one can establish that if every prime is a divisor of W and $Q = \pm 1$, then some term of W is 0 and so it is essentially the Lucas sequence $\cdots, 0, 1, P, \cdots$ associated with $f(x)$. Is this result true for arbitrary Q ?

REFERENCES

1. K. Mahler, "Eine arithmetische Eigenshaft der Taylor — koeffizienten rationaler Funktionen," Proc. Amsterdam Acad., 38 (1935), pp. 50-60.
2. K. Mahler, "A Remark on Recursive Sequences," J. Indian Math. Soc. (Dehli) 1.
3. M. Ward, "Prime Divisors of Second-Order Recurring Sequences," Duke Math. J., 21 (1954), pp. 607-614.
4. M. Ward, "The Laws of Apparition and Repetition of Primes in a Cubic Recurrence," Trans. Amer. Math. Soc., 79 (1955), pp. 72-90.