LINEAR RECURRENCES OF ORDER TWO

R. R. LAXTON

(Received 22 February 1966)

1. Introduction

Let $\{f(n)\}$ be a linear recurrence of order two, i.e.,

(1) $f(n+2) = af(n+1)+bf(n)$, $a, b \in Q$, for all positive integers n.

Its companion polynomial is $G(y) = y^2-ay-b$. We assume that none of its roots or ratios of roots are roots of unity. A problem is to determine an upper bound for the number of positive integers n such that $f(n) = \alpha$, where α is a given algebraic number. It has been proved that such an upper bound exists which is independent of α but the bound is dependent on the particular linear recurrence. K. Mahler [3] has shown that the greatest prime divisor of $f(n)$ tends to infinity with n. More recently in [4] he has proved that if a and b are integers and that $(a, b) = 1$, $|b| \geqq 2$ and $G(y)$ has complex conjugate roots, then for every $\varepsilon > 0$ and all sufficiently large n, $|f(n)| > |b|^{(1-\varepsilon)n/2}$; the same is true if the contributions of finitely many prime factors from $f(n)$ is omitted. One assumes that an upper bound exists which is independent of both α and the particular linear recurrence; indeed it is conjectured that this bound is 5 (see the article [5] of Morgan Ward, and the references contained therein).

Denote by $P(G)$ the set of primes $p \in Q$ such that the coefficients a, b of $G(y)$ are p-adic integers and the constant term b is a p-adic unit. We prove

THEOREM. *Let $\{f(n)\}$ be a linear recurrence of order two with companion polynomial $G(y) = y^2-ay-b \in Q[y]$ whose roots and ratios of roots are not roots of unity. Then for any algebraic number α, $f(n) = \alpha$ has at most M positive rational integral solutions n, where*

$$M = \min_{p \in P(G)} M_p \quad \text{and} \quad M_p = \begin{cases} 8 \text{ if } p = 2, \\ 10 \text{ if } p = 3, \\ p^2 \text{ if } p \neq 2, 3. \end{cases}$$

We use the p-adic method of Skolem.

2. Reduction to a $\mathfrak{p}$-adic problem

Let the roots of $G(y) = 0$ be β_1 and β_2. None of β_1, β_2, β_1/β_2 or β_2/β_1 are roots of unity. Since $\beta_1 \neq \beta_2$, we can write

$$f(x) = \sum_{j=1}^{2} A_j \beta_j^x, \tag{3}$$

where A_1 and A_2 are algebraic numbers (see [1]).

Let $p \in P(G)$, K be the field generated by β_1, β_2, A_1 and A_2 over Q and $K_\mathfrak{p}$ be the completion of K at a prime $\mathfrak{p}$ of K lying over p in Q. Put $\mathfrak{p} \cap Q(\beta) = \mathfrak{p}_1$ and let Q_1 denote the completion of $Q(\beta)$ at $\mathfrak{p}_1$. $\mathfrak{D}_\mathfrak{p}$ denotes the ring of $\mathfrak{p}$-adic integers in $K_\mathfrak{p}$. Let π be a uniformizing element of K and π_1 a uniformizing element of Q_1; thus $\mathfrak{p} = (\pi)$ in K and $\mathfrak{p}_1 = (\pi_1)$ in Q_1.

The normalized valuation of $K_\mathfrak{p}$ induced by $\mathfrak{p}$ will be denoted by $|\ |$; this valuation induces a valuation in each of the fields Q_1 and Q_p and $|p| = 1/p$. There exists a positive integer t such that $|\pi^t| = |\pi_1|$, a positive integer e such that $|\pi_1^e| = |p|$ and a positive integer f which is the degree of the residue class field $Q_1/\mathfrak{p}_1$ over Q/p. We know that $ef = 1$ or 2.

If m is $(p^f-1)p^{e-1}$ when $p \neq 2$ and is $(p^f-1)p^e$ when $p = 2$, then $\beta_1^m \equiv \beta_2^m \equiv 1 \pmod{\pi^{Wte}}$, where $W = 1$ when $p \neq 2$ and $W = 2$ when $p = 2$. Therefore we may assume that q is the *least positive integer* when $p \neq 2$ and the *least positive integer of the form* rp when $p = 2$ such that

$$\beta_1^q \equiv \beta_2^q \equiv 1 \pmod{\pi^{Wte}}. \tag{4}$$

Put

$$\delta_i = \beta_i^q \text{ for } i = 1, 2. \tag{5}$$

Then δ_1 and δ_2 are $\mathfrak{p}$-adic units and δ_1^x, δ_2^x are defined for all $x \in \mathfrak{D}_\mathfrak{p}$. Furthermore, the $\mathfrak{p}$-adic logarithms $\log \delta_1$, $\log \delta_2$ are defined and are $\mathfrak{p}$-adic integers.

Put

$$\delta_i = 1+\gamma_i\pi^S, \text{ where } \gamma_i \in \mathfrak{D}_\mathfrak{p}, \text{ for some } S \in Z^+. \tag{6}$$

Because β_i is not a root of unity $\delta_i \neq 1$ and so we may assume that either γ_1 or γ_2 is not congruent to zero modulo π; assume that

$$\gamma_1 \not\equiv 0 \pmod{\pi}. \tag{7}$$

Clearly $|\pi^S| \leqq |\pi^{Wte}| = |p^W|$. It follows that

$$\log \delta_i = \sum_{r=1}^{\infty} (-1)^{r-1} \gamma_i^r \frac{\pi^{Sr}}{r} = \pi^S \left\{ \gamma_i + \pi^S \sum_{r=2}^{\infty} (-1)^{r-1} \gamma_i \frac{\pi^{Sr-2}}{r} \right\}$$

and, as

https://doi.org/10.1017/S1446788700005139 Published online by Cambridge University Press

$$\left| \sum_{r=2}^{\infty} (-1)^{r-1} \gamma_i \frac{\pi^{Sr-2}}{r} \right| \leqq 1$$

by our choice of W, that

$$|\log \delta_1| = |\pi^S|, \ |\log \delta_2| \leqq |\pi^S|. \tag{8}$$

Let α be an algebraic number. We wish to determine an upper bound for the number of rational integral solutions x of

$$f(x, \alpha) \equiv A_1\beta_1^x + A_2\beta_2^x - \alpha = 0. \tag{9}$$

It is clear that we may assume that *both* A_1 and A_2 are not zero.

If x is a rational integer we may write $x = i+qy$ for some unique $y \in Z$ and i, $0 \leqq i < q$. If x is a solution of (9), then y is a rational integral solution of one of

$$g_i(y, \alpha) \equiv B_{1i}\delta_1^y + B_{2i}\delta_2^y - \alpha = 0, \qquad i = 0, 1, \cdots, q-1, \tag{10}$$

where $B_{ji} = A_j\beta_j^i$ for $i = 0, 1, \cdots, q-1$ and $j = 1, 2$. Therefore a rational integral solution of (9) gives rise to one and only one rational integral solution of one of the equations (10). Consequently we need only consider equations of the form (10). Furthermore, our upper bound for the number of rational integral solutions of the equations of the form (10) will be independent of the B_{ji} and α. We multiply (9) throughout by a power of π and take the A_i's, and so the B_{ji}'s, and α to be $\mathfrak{p}$-adic integers and at least one of B_{1j}, B_{2j}, α to be a $\mathfrak{p}$-adic unit. We note that $|B_{1j}| = |A_1|$ and $|B_{2j}| = |A_2|$ for all $j = 0, \cdots, q-1$.

3. The $\mathfrak{p}$-adic analysis

We have to determine an upper bound for the number of $\mathfrak{p}$-adic integral solutions y of the equation

$$g(y, \alpha) \equiv B_1\delta_1^y + B_2\delta_2^y - \alpha = 0, \tag{11}$$

where B_1, B_2 and α are $\mathfrak{p}$-adic integers with at least one a $\mathfrak{p}$-adic unit, B_1 and B_2 are non-zero and δ_1, δ_2 are $\mathfrak{p}$-adic units with the properties described in § 2.

Assume that (11) has one rational integral solution; then by a change of co-ordinates, if necessary, we may assume that this solution is $y = 0$ (this will involve multiplying the coefficients B_1 and B_2 by $\mathfrak{p}$-adic units only). In this new coordinate system

$$B_1 + B_2 - \alpha = 0. \tag{12}$$

We divide equation (11) by δ_2^y to obtain

$$h(y, \alpha) \equiv B_1 \left(\frac{\delta_1}{\delta_2}\right)^v + B_2 - \alpha(\delta_2^{-1})^v = 0; \tag{13}$$

now $h(y, \alpha) = 0$ if and only if $g(y, \alpha) = 0$.

Since $h(0, \alpha) = 0$, we can expand $h(y, \alpha)$ as a $\mathfrak{p}$-adic power series in y;

$$h(y, \alpha) \equiv \sum_{r=1}^{\infty} \left(B_1(\log \delta_1/\delta_2)^r - \alpha\ (\log \delta_2^{-1})^r\right) \frac{y^r}{r!}. \tag{14}$$

The coefficient of y^r in this expansion has valuation

$$|(B_1\ (\log \delta_1/\delta_2)^r - \alpha\ (\log \delta_2^{-1})^r)/r!\ | \leqq |\pi^{Sr}/r!| \leqq |p^{Wr}/r!|,$$

which has value $\leqq 1$ and tends to zero as $r \to \infty$. Therefore the expansion (14) converges for all $y \in \mathfrak{D}_\mathfrak{p}$.

We will determine an upper bound for the number of $\mathfrak{p}$-adic integral solutions of $h(y, \alpha) = 0$ with the aid of Strassman's lemma. This states that if $h(x) = \sum_{r=0}^{\infty} \gamma_v x^v$ has $\gamma_v \in \mathfrak{D}_\mathfrak{p}$, converges for all $x \in \mathfrak{D}_\mathfrak{p}$ and is non-zero for some $y \in \mathfrak{D}_\mathfrak{p}$, then $h(x)$ has at most $l = \{\max v$ for which $|\gamma_v|$ is maximal$\}$ zeros in $\mathfrak{D}_\mathfrak{p}$ (see [1]). We will see that in our case $l \leqq 2$ by comparing the coefficients of y and y^2 with the coefficients of y^r for $r \geqq 3$.

Put $a = B_1 \log \delta_1/\delta_2$ and $b = \alpha \log \delta_2^{-1}$; then the coefficients of y in (14) is $a - b$ and that of y^2 is (apart from a factor of 1/2) $[a(\log \delta_1/\delta_2) - b\ (\log \delta_2^{-1})]$. Now $a \neq 0$ (for $B_1 \neq 0$ and $\log \delta_1/\delta_2 \neq 0$ as β_1/β_2 is not a root of unity) and so we may put $\text{Max}\ (|a|, |b|) = |\pi^R|$; clearly $|\pi^R| \leqq |\pi^S|$.

Assume that

$$\begin{cases} a - b \equiv 0 \pmod{\pi^{R+1}} \\ a\ (\log \delta_1/\delta_2) - b\ (\log \delta_2^{-1}) \equiv 0 \pmod{\pi^{R+S+1}} \end{cases} \tag{15}$$

If we put $a' = a/\pi^R$, $b' = b/\pi^R$, $h_1 = (\log \delta_1/\delta_2)/\pi^S$ and $h_2 = (\log \delta_2^{-1})/\pi^S$, then all the elements a', b', h_1 and h_2 are $\mathfrak{p}$-adic integers and at least one of a', b' is a $\mathfrak{p}$-adic unit. Therefore the simultaneous equations

$$\begin{cases} Z_1 - Z_2 \equiv 0 \pmod{\pi} \\ Z_1 h_1 - Z_2 h_2 \equiv 0 \pmod{\pi} \end{cases}$$

have a non-trivial solution $(\text{mod } \pi)$ whereas its determinant of coefficients is

$$\begin{aligned} \Delta = \begin{vmatrix} 1 & 1 \\ h_1 & h_2 \end{vmatrix} &= h_2 - h_1 = (\log \delta_2^{-1} - \log \delta_1/\delta_2)/\pi^S \\ &= (-\log \delta_2 - \log \delta_1 + \log \delta_2)/\pi^S = -\log \delta_1/\pi^S, \end{aligned}$$

which is a $\mathfrak{p}$-adic unit by (8). Consequently the simultaneous congruences of (15) are impossible, therefore either the coefficient of y in (14) is not congruent to 0 $(\text{mod } \pi^{R+1})$ or the coefficient of y^2 in (14) is not congruent to 0 $(\text{mod } \pi^{R+S+1})$.

However, the coefficient C_r of y^r in (14) for $r \geqq 3$ has valuation

$$|(B_1 (\log \delta_1/\delta_2)^r - \alpha (\log \delta_2^{-1})^r)/r!| \leqq |\pi^{R+S(r-1)}| \left|\frac{1}{r!}\right|$$

$$\leqq |\pi^{R+S}| \left|\frac{\pi^{S(r-2)}}{r!}\right| \leqq |\pi^{R+S}| \left|\frac{\mathfrak{p}^{W(r-2)}}{r!}\right|.$$

If $\mathfrak{p} \neq 3$, $|C_r| \leqq |\pi^{R+S}|\ |\pi| < |\pi^{R+S}|$ for all $r \geqq 3$, whereas if $\mathfrak{p} = 3$, $|C_r| < |\pi^{R+S}|$ only for $r \geqq 4$. This follows from our choice of W in (4). Therefore, if $\mathfrak{p} \neq 3$ ($\mathfrak{p} = 3$) the valuations of all the coefficients of y^r for $r \geqq 3$ (resp. $r \geqq 4$) in the power series (14) are strictly less than the valuation of the coefficient of y or y^2. By Stassman's lemma, $h(y, \alpha) = 0$ can have at most two (resp. three) $\mathfrak{p}$-adic integral solutions and so each of the q equations of (10) can have at most two (resp. three) rational integral solutions.

Now if $G(y)$ splits over the local field $Q_\mathfrak{p}$ its roots β_1 and β_2 lie in $Q_\mathfrak{p}$, $|\pi_1| = 1/\mathfrak{p}$ and we have $q \leqq (\mathfrak{p}-1)$ for $\mathfrak{p} \neq 2$ and $q \leqq (\mathfrak{p}-1)\mathfrak{p} = 2$ for $\mathfrak{p} = 2$.

Therefore the above result shows that in this case the original equation (9) can have at most $2(\mathfrak{p}-1)$ rational integral solutions if $\mathfrak{p} \neq 2, 3$, at most 4 if $\mathfrak{p} = 2$ and at most $3(3-1) = 6$ if $\mathfrak{p} = 3$. These estimates are less than those we will obtain below for the case when $G(y)$ is irreducible over $Q_\mathfrak{p}$.

The coefficient of y^2 in (14) is $\frac{1}{2}\{B_1 (\log \delta_1/\delta_2)^2 - \alpha (\log \delta_2^{-1})^2\}$ which has valuation $\leqq |\pi^{R+S-n}|$, where $n = te$ if $\mathfrak{p} = 2$ and $n = 0$ if $\mathfrak{p} \neq 2$ (recall that $|\pi^{te}| = |\mathfrak{p}|$). Now if (14) is to have *two* $\mathfrak{p}$-adic integral solutions, then necessarily the coefficient of y must be congruent to 0 (mod π^{R+S-n}) i.e. $B_1 (\log \delta_1/\delta_2) - \alpha (\log \delta_2^{-1}) \equiv 0 \pmod{\pi^{R+S-n}}$.

Returning to (10), we see that if *two* different equations $g_k(y, \alpha) = 0$ and $g_l(y, \alpha) = 0$, $0 \leqq l < k \leqq q-1$, have *two* $\mathfrak{p}$-adic integral solutions, then

$$(16) \qquad \begin{cases} \beta_1^k \delta_1^K A_1 (\log \delta_1/\delta_2) - \alpha (\log \delta_2^{-1}) \equiv 0 \pmod{\pi^{R+S-n}} \\ \beta_1^l \delta_1^L A_1 (\log \delta_1/\delta_2) - \alpha (\log \delta_2^{-1}) \equiv 0 \pmod{\pi^{R+S-n}}, \end{cases}$$

where $A_1\beta_1^k\delta_1^K + A_2\beta_2^k\delta_2^K - \alpha = 0$, $A_1\beta_1^l\delta_1^L + A_2\beta_2^l\delta_2^L - \alpha = 0$ from (12). (It will be recalled that we changed coordinates at this point; K and L are rational integral solutions of $g_k(y, \alpha) = 0$ and $g_l(y, \alpha) = 0$ respectively.) Note that, with the previous notation, Max ($|a|$, $|b|$) is the same for all the forms $g_i(y, \alpha)$, $0 \leqq i \leqq q-1$, since the only difference in the coefficients of the different forms are multiples of $\mathfrak{p}$-adic units; in fact Max ($|A_1 \log \delta_1/\delta_2|$, $|\alpha \log \delta_2^{-1}|) = |\pi^R|$.

If $|A_1 \log \delta_1/\delta_2| < |\pi^R|$, then $|\alpha \log \delta_2^{-1}| = |\pi^R|$ and so (16) is impossible as $|\pi^{S-n}| \leqq |\pi^{Wte-n}| \leqq |\pi|$ for all primes $\mathfrak{p}$. Now suppose that $|A_1 \log \delta_1/\delta_2| = |\pi^R|$; then on subtracting the two equations in (16) we have

$$(\beta_1^k \delta_1^K - \beta_1^l \delta_1^L)\,(A_1 \log \delta_1/\delta_2) \equiv 0 \pmod{\pi^{R+S-n}}$$

and hence

$$\beta_1^k \delta_1^K - \beta_1^l \delta_1^L \equiv 0 \pmod{\pi^{S-n}}.$$

By (6), $\delta_1 \equiv 1 \pmod{\pi^S}$ and so this implies that $\beta_1^{(k-l)} \equiv 1 \pmod{\pi^{S-n}}$. But then $\beta_1^{(k-l)} \equiv 1 \pmod{\pi_1^{We-Ve}}$, where V is 1 if $p = 2$ and is 0 if $p \neq 2$.

We may assume that $G(y)$ is irreducible over Q_p, thus β_1 and β_2 are conjugate over Q_p. Consequently $\beta_1^{(k-l)} - 1$ and $\beta_2^{(k-l)} - 1$ are conjugate over Q_p, thus both $\beta_1^{(k-l)} \equiv 1 \pmod{\pi_1^{We-Ve}}$ and $\beta_2^{(k-l)} \equiv 1 \pmod{\pi_1^{We-Ve}}$.

If $p \neq 2$, $V = 0$ and, as $q > k-l > 0$, this contradicts our choice of q in (4). If $p = 2$, $We - Ve = 2e - e = e$ so that $\beta_i^{(k-l)} \equiv 1 \pmod{\pi_1^e}$ and therefore $\beta_i^{(k-l)2} \equiv 1 \pmod{\pi_1^{2e}}$. From our definition of q in (4) as the least positive integer of the form $r2$ such that $\beta_i^{r2} \equiv 1 \pmod{\pi^{2e}}$, we see that the only possibility is $k - l \equiv r \pmod{2r}$.

It follows that at most one of the q equations of (10) can have two (or possibly three if $p = 3$) $\mathfrak{p}$-adic integral solutions if $p \neq 2$ and at most two if $p = 2$. Therefore equation (9) can have at most $q+1$ rational solutions if $p \neq 2, 3$ and at most $q+2$ if $p = 2$ or 3. If $p \neq 2, 3$, $q+1 \leqq m+1 = (p^f-1)p^{e-1}+1 \leqq p^2$; if $p = 2$, $q+2 \leqq m+2 = (p^f-1)p^e+2 = (2^f-1)2^e+2 \leqq 8$, and if $p = 3$, $q+2 \leqq (p^f-1)p^{e-1}+2 \leqq 10$. This proves the theorem.

4. Remarks

In [5] Morgan Ward considered linear recurrences of order three with companion polynomials of the form $(y-a)(y-b)(y-c)$, where $abc \neq 0$, a, b, c rational integers. In non-degenerate cases, it is known that 0 can occur at most three times in such a recurrence, but Ward conjectured that the correct answer is two. The above method shows that this is correct when $a \equiv b \equiv c \equiv 1 \pmod 4$.

In [2] Nagell has considered the diophantine equation $f(x, y) = 1$, where $f(x, y)$ is an irreducible, binary, quartic form in $Z[x, y]$, $f(x, 1) = 0$ has no real roots and the extension $Q(\theta)$ (where $f(\theta, 1) = 0$) has a quadratic subfield. He has shown that such an equation has at most six rational integral solutions. In the remaining case when $Q(\theta)$ has no quadratic subfield, the field extension can contain no complex roots of unity. If α_1 is a fundamental unit of $Q(\theta)$ and α_2, α_3 are two of its conjugates, the problem can be reduced to one concerning an exponential equation of the form $a\alpha_1^z + b\alpha_2^z + c\alpha_3^z = 0$. Now one can use the above method to show that $|f(x, y)| = 1$ has at most thirty rational integral solutions (x, y) with $y \geqq 0$.

References

[1] Lewis, D. J., 'p-adic Methods'. Forthcoming article in M.A.A. series of 'Studies in Mathematics'.
[2] Nagell, T., 'Sur les representations de l'unite par les formes binaires biquadratique du premier rang', *Arkive for Matematik*, Bd 5, 33 (1965), 477–521.
[3] Mahler, K., Mathematica B (Zutphen), 3 (1934–35), 1–4.
[4] Mahler, K., 'A remark on recussive sequences'. *Journal of mathematical Sciences* (Delhi) I, 1 (1966), 12–17.
[5] Ward, M., 'Some diophantine problems connected with linear recurrences', *Report of the Institute in the Theory of Numbers*, University of Colorado, 1959, 250–257.

University of Sussex