ACTA ARITHMETICA
LVII (1991)

Arithmetical study of recurrence sequences

by

M. MIGNOTTE (Strasbourg) and N. TZANAKIS* (Iraklion)

Introduction. Arithmetical properties of linear recurrence sequences have been extensively studied in recent years.

The problems considered are: lower bounds (see [Ma], [Mi1], [M.S.T.],...), explicit computation of the zeros (see [Mi2]), bounds for the multiplicities (see [B.T.], [Be], [Ku]), lower bounds for $P(u_n)$ (see [Ste], [Sho],...), explicit computations of the repetitions (see [Mi3]),...

Several main tools are used in these studies: p-adic analysis (e.g. in [Ku] and [Mi2]), hypergeometric functions (e.g. in [B.T.]), linear forms in logarithms (e.g. in [Mi1], [M.S.T.], [Mi3],...), theorems on diophantine approximation of algebraic numbers (Roth–Ridout theorem in [Ma], Roth–Schmidt–Schlickewei theorem in [Ev] and [P.Sch.]). Among these tools the only one which automatically leads to "effective" results is the theory of lower bounds for linear forms in logarithms.

The second part of the survey [C.M.P.] is devoted to the arithmetical study of linear recurrences. This is also the subject of several chapters of the book [Sh.T.].

Many of these problems are much easier for binary sequences than for ternary ones. Indeed, several problems on ternary recurrence sequences remain open.

In Section I of the present paper we expose some preliminary facts concerning a general linear recurrence sequence (u_n). In Section II we develop a practical and easily applicable method, based on p-adic arguments, for solving (in the unknown n) an equation of the form $u_n = c$ where c is a given rational integer. In Section III we consider equations of the form $u_n = \pm p_1^{y_1} \ldots p_t^{y_t}$ in the unknowns $(n, y_1, \ldots, y_t)$, where $\{p_1, \ldots, p_t\}$ is a fixed set of prime numbers. We propose two elementary methods for finding upper

---

* Most of this work has been done while the second-named author held a visiting research position at the University of Strasbourg.

bounds for the exponents $y_1, \ldots, y_t$ so that the solution of the above equation is reduced to the solution of a finite number of equations of the type discussed in Section II. These elementary methods depend of the existence of some auxiliary primes possessing certain properties and, in this sense, they are based on *ad hoc* arguments. Nevertheless, it turns out that they work in every particular case we studied. In Sections II and III we give several numerical examples.

Among ternary linear recurrence sequences, it seems that Berstel's sequence (b_n), which is defined by $b_0 = b_1 = 0$, $b_2 = 1$, $b_n = 2b_{n-1} - 4b_{n-2} + 4b_{n-3}$ for $n \geqslant 3$, plays a very special rôle. Firstly, it is the only known example of a non-degenerate ternary linear recurrence sequence which has six zeros (by definition, a non-degenerate linear recurrence sequence has only finitely many zeros). It was proved in [Mi2] that it contains exactly six zeros. Beukers has just proved that six is the right upper bound for the number of zeros of non-degenerate ternary recurrence sequences of integers. Secondly, Berstel's sequence contains many repetitions, indeed it was proved in [Mi4] that the equation $b_m = \pm b_n$, for rational integers $m, n \in \boldsymbol{Z}$, has exactly 21 solutions (m, n) with $m < n$, and these solutions were explicitly computed. For the problem studied here, i.e. the equation $u_n = \pm 2^r 3^s$, it seems again that Berstel's sequence has remarkable properties: we can prove that there are exactly 44 solutions (n, r, s).

I. Preliminaries. We consider a kth order linear recurrence sequence (u_n) defined by

$$u_0 = c_0, \ \ldots, \ u_{k-1} = c_{k-1}, \ u_{n+k} = a_1 u_{n+k-1} + \ldots + a_k u_n, \quad n = 0, 1, 2, \ldots,$$

under the following assumptions:

(i) $c_0, \ldots, c_{k-1}$ and $a_1, \ldots, a_k$ are given rational numbers, $a_k \neq 0$,

(ii) the polynomial $g(X) = X^k - a_1 X^{k-1} - \ldots - a_{k-1} X - a_k$ has k distinct roots which we denote by $\omega_1, \ldots, \omega_k$.

Under the above assumptions it is a well-known fact (see [C.M.P.] for example) that the general term u_n of the recurrence sequence is equal to

$$u_n = \sum_{i=1}^{k} \alpha_i \omega_i^n, \tag{1}$$

where each α_i belongs to the field $\boldsymbol{Q}(\omega_1, \ldots, \omega_k)$, and has the shape: algebraic integer $\times (D(g))^{-1/2}$, where $D(g)$ is the discriminant of the polynomial $g(X)$.

Note that formula (1) permits us to extend the definition of u_n to negative n: if we put $u'_n = u_{-n}$ (for $n = 0, 1, 2, \ldots$), we have

$$u'_{n+k} = -(a_{k-1}/a_k) u'_{n+k-1} - \ldots - (a_1/a_k) u'_{n+1} + (1/a_k) u'_n.$$

From now on we will consider u_n for $n \in \boldsymbol{Z}$.

For the study of (u_n) we will work p-adically with an odd prime p which fulfils the following conditions:

(P1) $$|a_i|_p \leqslant 1 \quad (i = 1, \ldots, k); \quad |a_k|_p = 1;$$

(P2) $$|D(g)|_p = 1;$$

(P3) $$|u_j|_p \leqslant 1 \quad (j = 0, \ldots, k-1).$$

Note that these conditions imply $|\omega_i|_p \leqslant 1$ and $|\alpha_i|_p \leqslant 1$ for $i = 1, \ldots, k$.

Let p be a prime satisfying these conditions. Choose a positive integer S such that $\omega_i^S \equiv A \pmod p$, for some $A \in \boldsymbol{Z}$ and all $i \in \{1, \ldots, k\}$ and take the p-adic $(p-1)$th root of a unity which satisfies $a \equiv A \pmod p$. Then $\omega_i^S = a(1+p\beta_i)$, $i = 1, \ldots, k$, for some $\beta_1, \ldots, \beta_k$ integral over the ring $\boldsymbol{Z}_p$ (of p-adic integers). Let m, $N \in \boldsymbol{Z}$. Then

(2) $$u_{m+NS} = \sum_{i=1}^{k} \alpha_i \omega_i^{m+NS} = \sum_{i=1}^{k} \alpha_i \omega_i^m a^N (1+p\beta_i)^N$$
$$= a^N \sum_{r=0}^{\infty} \sum_{i=1}^{k} \alpha_i \omega_i^m \binom{N}{r} p^r \beta_i^r = a^N \sum_{r=0}^{\infty} \binom{N}{r} p^r b_{mr},$$

where

$$b_{mr} = \sum_{i=1}^{k} \alpha_i \omega_i^m \beta_i^r.$$

Note that $b_{mr} \in \boldsymbol{Q}$, $|b_{mr}|_p \leqslant 1$ for all m, r and $b_{m0} = u_m$ for all m. In particular,

(3) $$u_{m+NS} \equiv a^N u_m \equiv A^N u_m \pmod p.$$

II. Solution of the equation $u_n = c$. We want to find all the indices n for which $u_n = c$, where c is a given rational number. Very often, in practice, we know a finite set $\mathscr{M}$ such that $u_m = c$ for every m in $\mathscr{M}$ and we want to prove that $\mathscr{M}$ is indeed the set of **all** indices m such that $u_m = c$.

THEOREM 1. *Let S and A be as above. Suppose we have chosen A in such a way that the orders of A mod p and mod p^2 have the same value R. Suppose that either $c \not\equiv 0 \pmod p$ or $c = 0$. Let $\mathscr{P}$ be a complete system of residues modulo S such that $\mathscr{P} \supseteq \mathscr{M}$ and which satisfies the following conditions:*

(i) $u_m = c$ for every m in $\mathscr{M}$,

(ii) if $u_n \equiv cA^r \pmod p$ for some $r \in \{0, 1, \ldots, R-1\}$, then $n \in \mathscr{M}$,

(iii) $u_{m+S} \not\equiv Au_m \pmod{p^2}$ for every $m \in \mathscr{M}$.

Then $u_n = c$ implies $n \in \mathscr{M}$.

Proof. Let a be the p-adic $(p-1)$th root of unity such that $A \equiv a \pmod p$. Note that our choice of A implies $A \equiv a \pmod{p^2}$.

Suppose that $u_n = c$. Take $m \in \mathscr{P}$ such that $n \equiv m \pmod S$ and put $n = NS+m$ where $N \in \boldsymbol{Z}$. From (3), we have $u_n = u_{m+NS} \equiv A^N u_m \pmod p$ and condition (ii) implies $m \in \mathscr{M} \Rightarrow u_m = c$. Thus, $c \equiv A^N c \pmod p$. Suppose $c \not\equiv 0 \pmod p$. Then $A^N \equiv 1 \pmod p$, $a^N = 1$ and $u_n - a^N u_m = c - c = 0$. If $c = 0$, then automatically $u_n - a^N u_m = 0$. So, in both cases, using (2), we are left with

$$0 = a^N \sum_{r=1}^{\infty} \binom{N}{r} p^r b_{mr}.$$

If $N \neq 0$ then, after division by $a^N Np$, we get

$$0 = b_{m1} + \sum_{r=2}^{\infty} \binom{N-1}{r-1} \frac{p^{r-1}}{r} b_{mr}. \tag{4}$$

Since p is an odd prime, $|p^{r-1}/r|_p \leqslant 1$ for all $r \geqslant 2$, and (4) implies that $p | b_{m1}$. It follows from (2) with $N = 1$ that $apb_{m1} = u_{m+S} - au_m$, hence $p^2 | u_{m+S} - au_m$. Together with $A \equiv a \pmod{p^2}$ this yields $p^2 | u_{m+S} - Au_m$, contradicting condition (iii). Therefore, we necessarily have $N = 0$ and consequently $n = m \in \mathcal{M}$, as claimed.

We shall give several applications of Theorem 1 (see Examples 1 to 4 below).

Remark. In most cases it is preferable to choose a prime p among those that split completely in the field K, because for such p the value of S divides $p-1$, while, for all other primes, S is generally of the order of p^m with $m \geqslant 2$. In all the examples given in the present paper our prime p splits completely in K.

EXAMPLES. 1. $u_0 = 0$, $u_1 = 1$, $u_2 = 0$, $u_{n+3} = -u_{n+2} - u_{n+1} + u_n$. We want to solve

$$u_n = 0, \quad n \in \mathbf{Z}. \tag{5}$$

We apply Theorem 1 with $\mathcal{M} = \{0, 2\}$, $p = 103$, $S = 17$, $\mathcal{P} = \{0, 1, \ldots, 16\}$. The only values of n in the range $0 \leqslant n \leqslant 16$ for which $u_n \equiv 0 \pmod{103}$ are those of the set $\mathcal{M}$. Thus, condition (ii) of Theorem 1 holds; u_{17} and u_{19} are not divisible by 103^2, which shows that condition (iii) is also true. Conclusion: (5) is true exactly for $n = 0, 2$.

2. $u_0 = u_1 = 0$, $u_2 = 1$, $u_{n+3} = -u_{n+2} - u_{n+1} + u_n$. In this case, we want to prove that

$$u_n = 0, \ n \in \mathbf{Z} \quad \text{implies} \quad n \in \{0, 1, 4, 17\}. \tag{6}$$

Thus, in this example $\mathcal{M} = \{0, 1, 4, 17\}$.

Note that for the application of Theorem 1 we cannot work with $p = 103$, because, for this prime, $S = 17$ and $u_{17} = 0$, which shows that condition (iii) is not fulfilled. We work with $p = 163$. Then $S = 54$ and we can take $\mathcal{P} = \{0, 1, 2, \ldots, 53\}$. With the aid of a computer (or even of a pocket-calculator) one sees that the only values of n in the range $0 \leqslant n \leqslant 53$ for which u_n is divisible by 163 are those belonging to $\mathcal{M}$, and then that for $n \in 54 + \mathcal{M} = \{54, 55, 58, 71\}$ the integer u_n is not divisible by 163^2. According to Theorem 1, these observations imply that (6) is true iff $n \in \mathcal{M}$.

3. Same recurrence as in Example 1. We want to solve

$$u_n = -2, \quad n \in \mathbf{Z}. \tag{7}$$

We apply Theorem 1 with the following choices: $p = 103$, $S = 17$, $A = 56$, $R = 3$, $\mathcal{M} = \{6, 12\}$ and $\mathcal{P} = \{0, 1, \ldots, 16\}$. It is easily checked that conditions (i) to (iii) of Theorem 1 hold, which proves that (7) is true exactly for $n \in \mathcal{M}$.

4. Same recurrence as in Example 1. We want to solve

$$u_n = 2, \quad n \in \mathbf{Z}. \tag{8}$$

We take $p = 103$, $S = 17$, $A = 56$, $\mathcal{M} = \{-2, 4\}$ and $\mathcal{P} = \{-2, -1, 0, 1, \ldots, 14\}$. It is easily checked that for $0 \leqslant n \leqslant 16$ the only values for which $u_n \equiv 2 \cdot 56^r \pmod{103}$ for some r are $n = 4, 15$ [in fact $r \in \{0, 1, 2\}$ since $R = 3$] and therefore the only values n in $\mathcal{P}$ for which the above congruence is valid are those belonging to $\mathcal{M}$. Thus, condition (ii) holds and it is straightforward to check also the validity of (i) and (iii). Thus, the only solutions to equation (8) are $n = -2, 4$.

III. Solution of the equation $u_n = \pm q_1^{y_1} \ldots q_r^{y_r}$. In this equation $q_1, \ldots, q_r$ are given prime numbers and $y_1, \ldots, y_r$ are unknown non-negative integers. A general and practical method of solution in the case of a second order recurrence sequence has been developed by Pethö and de Weger [P.W.] and de Weger [We]. For higher order recurrence sequences the development of an analogous method is a very difficult task. However, if a specific equation is given, then a practical method for finding explicitly all its solutions can be based on the following result.

THEOREM 2. *Let p, q be two different primes. Let S be a positive rational integer such that $\omega^S \equiv A \pmod p$, with $A \in \mathbf{Z}$. Put $\mathcal{M} = \{m \in \mathbf{Z};\, u_m = 0\}$ and suppose that the following condition is satisfied: there exists a positive rational integer v such that*

$$u_n \equiv 0 \pmod{q^v} \Rightarrow \exists m \in \mathcal{M} \text{ such that } n \equiv m \pmod S.$$

Then $u_n \equiv 0 \pmod{q^v}$ implies that p divides u_n.

Proof. Suppose $u_n \equiv 0 \pmod{q^v}$. Then, by hypothesis, there exists $m \in \mathcal{M}$ such that $n \equiv m \pmod S$. Put $n = m + NS$. We know that $u_n \equiv A^N u_m$ modulo p (see (3)). Since $u_m = 0$, this implies $u_n \equiv 0 \pmod p$, as claimed.

EXAMPLE 5. Let $u_0 = u_1 = 0$, $u_2 = 1$ and $u_{n+3} = -u_{n+2} - u_{n+1} + u_n$. We want to solve

$$u_n = \pm 2^s, \quad s \geqslant 0. \tag{9}$$

We first apply Theorem 2 with $q = 2$, $p = 7$, $S = 32$ ($A = 4$). We observe that

$$u_n \equiv 0 \pmod{2^4} \Rightarrow n \equiv 0, 1, 4, 17 \pmod S$$

and $0, 1, 4, 17 \in \mathcal{M}$. Therefore, by Theorem 2, if 16 divides u_n then 7 divides u_n. This means that, in relation (9), we must have $s \leqslant 3$: we only have to solve the eight equations $u_n = c$ for $c \in \{\pm 1, \pm 2, \pm 4, \pm 8\}$.

The sequence u_n is periodic modulo 53 with period-length 52. One verifies that we never have $u_n \equiv -2, -4, 8 \pmod{53}$: this excludes the values $c = -2, -4, 8$. For the values $c = \pm 1, 2, 4$ we apply Theorem 1 with $p = 53$, $T = 52$, $\mathscr{P} = \{-4, -3, -2, \ldots, 47\}$ and $\mathscr{M} = \{3\}$ if $c = -1$, $\mathscr{M} = \{-2, -1, 2, 7\}$ if $c = 1$, $\mathscr{M} = \{-3, 5\}$ if $c = 2$, $\mathscr{M} = \{-4, 8\}$ if $c = 4$.

Then conditions (i) and (ii) of Theorem 1 are satisfied. Also, an easy computation shows that condition (iii) of the same theorem holds too: we need only to compute the values u_{55}; $u_{50}, u_{51}, u_{54}, u_{59}$; u_{49}, u_{57}; u_{48}, u_{60} modulo 53^2 and check that they are $\not\equiv c \pmod{53^2}$ for $c = -1, 1, 2, 4$ respectively. Thus Theorem 1 implies that

$$u_n = -1 \Rightarrow n = 3; \qquad u_n = 1 \Rightarrow n = -2, -1, 2, 7,$$
$$u_n = 2 \Rightarrow n = -3, 5; \qquad u_n = 4 \Rightarrow n = -4, 8.$$

Finally, to solve the equation $u_n = -8$, we apply Theorem 1 with $p = 163$, $T = 162$, $\mathscr{P} = \{0, 1, \ldots, 161\}$ and $\mathscr{M} = \{9\}$ to see that $u_n = -8$ iff $n = 9$.

Final conclusion: the only solutions of $u_n = \pm 2^s$ are the following:

$$u_{-4} = 4,\ u_{-3} = 2,\ u_{-2} = 1,\ u_{-1} = 1,$$
$$u_2 = 1,\ u_3 = -1,\ u_5 = 2,\ u_7 = 1,\ u_8 = 4,\ u_9 = 8.$$

Remark. In certain cases, instead of applying Theorem 2, we work as follows (we keep the notations of Theorem 2): Suppose that q is relatively prime to a_k. Then (u_n) is a periodic sequence modulo q^v, for any positive integer v, with period-length Q, say. Moreover, suppose that (u_n) is a periodic sequence modulo some prime number $p \neq q$, with period-length equal to P, where $\gcd(P, Q)$ is not "very small". Then the relation $u_n \equiv 0 \pmod{q^v}$ restricts the values of the index n modulo Q – and therefore modulo P – to only a "few" possibilities, say $n = n_1, \ldots, n_k \pmod{P}$.

If we are lucky in our choice of the prime p, it can happen that p divides u_{n_j} for every index $j = 1, 2, \ldots, k$, and in this case we get the same conclusion as the one we obtained in Theorem 2, i.e.

$$u_n \equiv 0 \pmod{q^v} \Rightarrow u_n \equiv 0 \pmod{p}.$$

EXAMPLE. Let $u_0 = u_1 = 0$, $u_2 = 1$, $u_{n+3} = -u_{n+2} - u_{n+1} + u_n$. We want to solve

$$u_n = \pm 2^r. \tag{10}$$

Take $q^v = 2^4$ and $p = 7$, so that $P = 32$ and $Q = 48$, $\gcd(P, Q) = 16$. The relation $u_n \equiv 0 \pmod{q^v}$ implies $n \equiv 0, 1, 4, 17 \pmod{P}$; i.e. $n \equiv 0, 1, 4, 17 \pmod{16}$ (here $n_1 = 0$, $n_2 = 1$ and $n_3 = 4$). It turns out that $u_0 = u_1 = u_4 = 0$ (we need only the fact that u_0, u_1, u_4 are divisible by 7), which contradicts (10). We conclude therefore that $r \leqslant 3$ and then we solve (10) for these values of r, case by case, using the method of Section II.

IV. Study of Berstel's sequence. Based on the techniques developed in the previous sections and using some *ad hoc* tricks (which can be tried with many chances of success for analogous equations as well) we solved the equation

$$b_n = \pm 2^{y_1} \cdot 3^{y_2}, \qquad y_1, y_2 \in \mathbf{Z},$$

where (b_n) is Berstel's sequence: $b_0 = b_1 = 0$, $b_2 = 1$, $b_{n+3} = 2b_{n+2} - 4b_{n+1} + 4b_n$. The complete solution of this equation is given in the theorem below. The details of the proof will be published elsewhere (reprints available on request).

THEOREM. *The only solutions* (n, y_1, y_2) *of the equation*

$$b_n = \pm 2^{y_1} \cdot 3^{y_2}, \qquad n \in \mathbf{Z},$$

where $b_0 = b_1 = 0$, $b_2 = 1$, $b_{n+3} = 2b_{n+2} - 4b_{n+1} + 4b_n$, *are the* 44 *ones listed below.*

n	-26	-20	-13	-12	-11	-9	-8	-7	-6
b_n	$2^{-18}3^4$	$2^{-11}3$	$2^{-10}3^2$	$2^{-8}3$	2^{-6}	$2^{-7}3$	2^{-5}	$2^{-6}3$	2^{-4}

n	-5	-4	-3	-2	-1	2	3	5	7
b_n	2^{-4}	2^{-4}	2^{-3}	2^{-2}	2^{-2}	1	2	-2^2	2^4

n	8	9	10	11	12	14	15	16	17
b_n	2^4	-2^5	-2^6	2^6	2^8	$-2^8 3$	-2^9	2^{11}	$2^{10}3$

n	18	19	20	22	24	25	26	27	28
b_n	-2^{12}	$-2^{12}3$	2^{12}	2^{14}	-2^{17}	2^{18}	$2^{16}3^2$	$-2^{17}3$	-2^{21}

n	29	30	36	39	40	43	45	91
b_n	-2^{18}	$2^{21}3$	-2^{24}	$2^{25}3^3$	$2^{27}3^2$	$2^{28}3^2$	$2^{29}3^2$	$2^{60}3^4$

Acknowledgment. The authors would like to thank the referee whose comments considerably simplified the present paper.

References

[Be] F. Beukers, *The multiplicity of binary recurrences*, Compositio Math. 40 (1980), 251–267.

[B.T.] F. Beukers and R. Tijdeman, *On the multiplicity of binary complex sequences*, ibid. 51 (1984), 193–213.

[C.M.P.] L. Cerlienco, M. Mignotte et F. Piras, *Suites récurrentes linéaires, Propriétés algébriques et arithmétiques*, Enseign. Math. 33 (1987), 67–108.

[Ev] J. H. Evertse, *On sums of S-units and linear recurrences*, Compositio Math. 53 (1984), 225–244.

[Ku] K. Kubota, *On a conjecture of M. Ward I, II, III*, Acta Arith. 33 (1977), 11–28, 29–48, 99–109.

[Ma] K. Mahler, *A remark on linear recursive sequences*, J. Math. Sci. 1 (1966), 12–17.

[Mi1] M. Mignotte, *Suites récurrentes linéaires*, Sém. Delange–Pisot–Poitou, 15, 1973/74, Gr. ét. n° 14, 9 pages.

[Mi2] —, *A note on linear recursive sequences*, J. Austral. Math. Soc. Ser. A 20 (1975), 242–244.

[Mi3] —, *Une extension du théorème de Skolem–Mahler*, C.R. Acad. Sci. Paris Sér. A 288 (1979), 233–235.

[Mi4] —, *Détermination des répétitions d'une certaine suite récurrente linéaire*, Acta Math. Debrecen 33 (1986), 297–306.

[M.S.T.] M. Mignotte, T. Shorey and R. Tijdeman, *The distance between terms of an algebraic recurrence sequence*, J. Reine Angew. Math. 349 (1984), 63–76.

[P.Sch.] A. J. van der Poorten and H. P. Schlickewei, *The growth condition for recurrence sequences*, Report 82-0041, Macquarie University, N.S.W., Australia, 1982.

[P.W.] A. Pethő and B. M. M. de Weger, *Products of prime powers in binary recurrence sequences I, The hyperbolic case with an application to the generalized Ramanujan–Nagell equation*, Math. Comp. 47 (1986), 713–727.

[Sho] T. N. Shorey, *The greatest square-free factor of a binary recursive sequence*, Hardy-Ramanujan J., 6 (1983), 23–36.

[Sh.T.] T. N. Shorey and R. Tijdeman, *Exponential Diophantine Equations*, Cambridge Tracts in Math. 87, Cambridge Univ. Press, 1986.

[Ste] C. L. Stewart, *On the greatest prime factor of terms of a linear recurrence sequence*, Rocky Mountain J. Math., to appear.

[We] B. M. M. de Weger, *Products of prime powers in binary recurrence sequences II*, Math. Comp. 47 (1986), 729–739.

MATHÉMATIQUE
UNIVERSITÉ LOUIS PASTEUR
67084 Strasbourg, France

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF CRETE
Iraklion, Crete, Greece

Received on 12.6.1989
and in revised form on 7.12.1989 (1946)