BULLETIN OF THE POLISH
ACADEMY OF SCIENCES
MATHEMATICS
Vol. 67, No. 1, 2019

NUMBER THEORY

Local-global principles for recurrence sequences

by

A. SCHINZEL and M. SKAŁBA

Summary. A proof is given that if a non-degenerate recurrence sequence of the second order over the rationals with separable companion equation contains multiples of infinitely many terms of the Lucas sequence governed by the same recurrence, then it contains zero for an index of a suitable sign.

Our goal is to prove some new local-global principles for non-degenerate binary linear sequences with distinct eigenvalues. The main result is

THEOREM 1. *Let $P = a/c$, $Q = b/c^2$ with $a, b \in \mathbb{Z}$, $c, d \in \mathbb{N}$, $(a, b, c) = 1$, suppose that*

$$dx_0, dx_1 \in \mathbb{Z}, \qquad x_n = Px_{n-1} - Qx_{n-2},$$
$$u_0 = 0,\ u_1 = 1, \qquad u_n = Pu_{n-1} - Qu_{n-2},$$

and assume that $P^2 \neq 4Q$. If the sequence u_n is not degenerate and if the congruence

$$x_n \equiv 0 \pmod{c^{k-1}u_k} \tag{1}$$

is soluble in n for infinitely many positive integers k, then the equation $x_n = 0$ is soluble in integers n.

Proof. Let us put

$$L = \frac{a^2}{(a^2, b)}, \qquad M = \frac{b}{(a^2, b)}, \qquad K = L - 4M;$$
$$\alpha_0 = \frac{a + \sqrt{a^2 - 4b}}{2c}, \qquad \alpha_1 = \alpha_0 c, \qquad \alpha = \frac{\sqrt{L} + \sqrt{K}}{2};$$

2010 *Mathematics Subject Classification*: Primary 11B39.
Key words and phrases: recurrence sequences, local-global principle.
Received 20 December 2018.
Published online 14 February 2019.

DOI: 10.4064/ba8179-1-2019

$$\beta_0 = \frac{a - \sqrt{a^2 - 4b}}{2c}, \quad \beta_1 = \beta_0 c, \quad \beta = \frac{\sqrt{L} - \sqrt{K}}{2}.$$

The numbers

$$P_n(\alpha, \beta) = \frac{\alpha^n - \beta^n}{\alpha^{\delta_n} - \beta^{\delta_n}}, \quad \delta_n \in \{1, 2\},\ \delta_n \equiv n \pmod 2,$$

are called *Lehmer numbers*. We have

$$c^{k-1} u_k = \frac{\alpha_1^k - \beta_1^k}{\alpha_1 - \beta_1} = (a^2, b)^{(k-\delta_k)/2} a^{\delta_k - 1} P_k(\alpha, \beta). \tag{2}$$

The laws of appearance and repetition of primes p among Lehmer numbers [2, pp. 421–424] imply

$$\nu_p(P_k(\alpha, \beta)) \le a_p \log k + b_p, \tag{3}$$

where a_p and b_p are independent of k.

If $n = kq + r$ with $q, r \in \mathbb{Z}$, $|r| \le k/2$, we have

$$\alpha^k \equiv \beta^k \pmod{P_k(\alpha, \beta)},$$

hence

$$\alpha^{kq} \equiv \beta^{kq} \pmod{P_k(\alpha, \beta)}, \quad \alpha_1^{kq} \equiv \beta_1^{kq} \pmod{P_k(\alpha, \beta)}.$$

On the other hand,

$$x_n = \psi \alpha_0^n + \omega \beta_0^n, \quad \text{where } \psi, \omega \in \mathbb{C} \text{ are independent of } n,$$

hence by (1) and (2),

$$\beta_1^{kq} x_r \equiv 0 \pmod{P_k(\alpha, \beta)}, \quad (a^2, b)^{\lceil kq/2 \rceil} x_r \equiv 0 \pmod{P_k(\alpha, \beta)}. \tag{4}$$

Let $\varepsilon_r \in \{0, 1\}$, $\varepsilon_r \equiv r \pmod 2$, and

$$m = \frac{|P_k(\alpha, \beta)|}{(P_k(\alpha, \beta), (a^2, b)^{\lceil kq/2 \rceil})}.$$

We have $m \in \mathbb{Z}$ and by (4), $x_r \equiv 0 \pmod m$.

If $r \ge 0$, then

$$dc^r (a^2, b)^{(\varepsilon_r - r)/2} x_r \in \mathbb{Z},$$

$$dc^r (a^2, b)^{(\varepsilon_r - r)/2} x_r \equiv 0 \left(\bmod \frac{m}{(m, (a^2, b)^{(r - \varepsilon_r)/2})} \right)$$

and

$$dc^r (a^2, b)^{(\varepsilon_r - r)/2} x_r = \mathcal{O}(|\alpha|^r).$$

On the other hand, by (3) and Baker's estimate (see [1, Theorem 2.4]), for k large enough we have

$$m > |\alpha|^{k - \mathcal{O}(\log k)} > \mathcal{O}(|\alpha|^r).$$

If $r<0$, then

$$\frac{d\alpha_1^{|r|}\beta_1^{|r|}}{c^{|r|}}x_r\in\mathbb{Z},\qquad \frac{d\alpha_1^{|r|}\beta_1^{|r|}}{c^{|r|}}x_r\equiv 0\ \left(\mathrm{mod}\ \frac{(a^2,b)^{|r|}m}{(m,c^{|r|})}\right)$$

(here we use the condition $(a,b,c)=1$) and

$$\frac{d\alpha_1^{|r|}\beta_1^{|r|}}{c^{|r|}}x_r=\mathcal{O}(|\alpha_1|^{|r|}).$$

On the other hand, by (3) and Baker's estimate, for k large enough,

$$\frac{(a^2,b)^{|r|}m}{(m,c^{|r|})}>(a^2,b)^{|r|}|\alpha|^{k-\mathcal{O}(\log k)}>\mathcal{O}(|\alpha_1|^{|r|}).$$

In both cases $x_r=0$.

THEOREM 2. *Let $P\in\mathbb{Z}$, $Q=\pm1$, $d\in\mathbb{N}$, $c\in\mathbb{Q}$,*

$$dx_0,dx_1,dc\in\mathbb{Z},\qquad x_n=Px_{n-1}-Qx_{n-2},$$
$$u_0=0,\ u_1=1,\qquad u_n=Pu_{n-1}-Qu_{n-2}.$$

If $P^2\neq 4Q$ and if the congruence

$$x_n\equiv c\ (\mathrm{mod}\ u_k) \tag{5}$$

is soluble in n for infinitely many positive integers k, then the equation $x_n=c$ is soluble in integers n.

Proof. We retain the notation of the proof of Theorem 1 with the difference that now $n=2kq+r$, $|r|\le k$. For every positive integer n, dx_n and dc are integers, therefore the congruence (5) implies that $(dx_n-dc)/u_k\in\mathbb{Z}$. Since by (2), $u_k=\frac{\alpha^k-\beta^k}{\alpha-\beta}$, where $|\alpha|\ge|\beta|$ and the sequence u_k is non-degenerate, we have either $x_n=c$ or

$$\left|\frac{\psi\alpha^{r-k}+\omega\beta^r\alpha^{-k}-c\alpha^{-k}}{1-(\beta/\alpha)^k}\right|\ge\frac{1}{d\sqrt{P^2-4Q}}.$$

For a properly chosen sequence $k_1<k_2<\cdots$ at least one of the sequences $(|\psi\alpha^{r_j-k_j}|)_j$ or $(|\omega\beta^{r_j}\alpha^{-k_j}|)_j$ is bounded from below by some positive number. Since $\beta=Q\alpha^{-1}$ and $|\alpha|>1$ it follows that either $(k_j-r_j)_j$ or $(k_j+r_j)_j$ is bounded. In the first case $k_j-r_j=s$ for infinitely many j. The discrete sequence

$$y_j:=\frac{\psi\alpha^{-s}+\omega Q^{r_j}\alpha^{-r_j-k_j}-c\alpha^{-k_j}}{1-Q^{k_j}\alpha^{-2k_j}}=\frac{\psi\alpha^{-s}+\omega Q^{r_j}\alpha^{s-2k_j}-c\alpha^{-k_j}}{1-Q^{k_j}\alpha^{-2k_j}}$$

converges to $\psi\alpha^{-s}$ and therefore

$$\frac{\psi\alpha^{-s}+\omega Q^{r_j}\alpha^{s-2k_j}-c\alpha^{-k_j}}{1-Q^{k_j}\alpha^{-2k_j}}=\psi\alpha^{-s}\qquad\text{for } j\ge j_0.$$

This means

$$\psi Q^{k_j}\alpha^{-s} + \omega Q^{r_j}\alpha^{s} = c\alpha^{k_j} \quad \text{for } j \geq j_0,$$

which contradicts $|\alpha| > 1$ (by Theorem 1 the case $c = 0$ is settled). In the second case, $k_j + r_j = s$ for infinitely many j and the argument is analogous.

If (x_n) is a sequence considered in Theorem 1 then the following local-global principle follows immediately from the results of the first named author [3], [4].

If for almost all prime numbers p (in the sense of Dirichlet density) the congruence

$$x_n \equiv 0 \pmod{p}$$

is soluble in $n \in \mathbb{N}$ then there exists $n \in \mathbb{Z}$ satisfying $x_n = 0$. If $Q = \pm 1$ and $c \in \mathbb{Q}$, the same applies to the congruence $x_n \equiv c \pmod{p}$ and the equation $x_n = c$.

The sequence (p_k) of primes is thus a universal testing sequence in opposition to our sequence (u_k) of Lucas numbers which is selected to satisfy the same recurrence as the sequence (x_n) under consideration. Besides, we can choose P non-integral. On the other hand, the advantage of our principle is that it requires only an infinite number of k's (without any requirements on density).

References

[1] G. Everest, A. van der Poorten, I. Shparlinski and T. Ward, *Recurrence Sequences*, Math. Surveys Monogr. 104, Amer. Math. Soc., 2003.

[2] D. H. Lehmer, *An extended theory of Lucas' functions*, Ann. of Math. (2) 31 (1930), 419–448.

[3] A. Schinzel, *On power residues and exponential congruences*, Acta Arith. 27 (1975), 397–420; also in: Selecta, Vol. 2, Eur. Math. Soc., 2007, 915–938.

[4] A. Schinzel, *On simple linear recurrences*, in: Number Theory—Diophantine Problems, Uniform Distribution and Applications, Springer, Cham, 2017, 381–389.

A. Schinzel
Institute of Mathematics
Polish Academy of Sciences
Śniadeckich 8
00-656 Warszawa, Poland
E-mail: schinzel@impan.pl

M. Skałba
Institute of Mathematics
University of Warsaw
Banacha 2
02-097 Warszawa, Poland
E-mail: skalba@mimuw.edu.pl