

## On Ternary Integral Recurrences

by

A. SCHINZEL

**Summary.** We prove that if  $a, b, c, d, e, m$  are integers,  $m > 0$  and  $(m, ac) = 1$ , then there exist infinitely many positive integers  $n$  such that  $m \mid (an + b)c^n - de^n$ . Hence we derive a similar conclusion for ternary integral recurrences.

An integral recurrence of order  $k$  is given by the formula

$$u_n = c_1 u_{n-1} + c_2 u_{n-2} + \cdots + c_k u_{n-k},$$

where  $c_i$  and  $u_i$  ( $1 \leq i \leq k$ ) are integers.

The aim of this paper is to prove

**THEOREM.** *For every essentially ternary integral recurrence sequence  $u_n$  the companion polynomial of which has a double zero, there exists an integer  $D > 0$  such that for all integers  $m$  prime to  $D$  infinitely many terms  $u_n$  are divisible by  $m$ .*

For simple integral recurrence sequences  $u_n$  of any order, there is a conjecture of Skolem [3] (see also Skolem [4, p. 56] and Schinzel [1]) that if for every integer  $m > 0$  there is  $u_n$  divisible by  $m$ , then there is  $n$  with  $u_n = 0$ . It follows from the above theorem that a similar assertion is false for non-simple integral recurrences, e.g. for  $u_n = n + 2^n$ .

The proof of the Theorem is based on four lemmas. In the course of the proofs  $p$  denotes a prime,  $\mathbb{Z}_p$  and  $\mathbb{Q}_p$  the ring of  $p$ -adic integers and the field of  $p$ -adic numbers, respectively,  $e_p = \max\{1, 4 - p\}$ , and if  $z \in \mathbb{Q}_p \setminus \{0\}$ , then  $\text{ord}_p z = \max\{\alpha \in \mathbb{Z} : p^{-\alpha} z \in \mathbb{Z}_p\}$ .

**LEMMA 1.** *If  $z, w \in \mathbb{Q}_p$ ,  $\min\{\text{ord}_p(z - 1), \text{ord}_p(w - 1)\} \geq e_p$  and  $\log_p z$  is the  $p$ -adic logarithm of  $z$ , then*

$$(1) \quad \text{ord}_p(z - w) = \text{ord}_p(\log_p z - \log_p w).$$

2010 *Mathematics Subject Classification:* Primary 11B37.

*Key words and phrases:* ternary recurrence,  $p$ -adic logarithm.

*Proof.* From the power series expansion we have

$$\text{ord}_p(\log_p z - \log_p w) = \text{ord}_p\left(\log_p \frac{z}{w}\right) = \text{ord}_p\left(\frac{z}{w} - 1\right) = \text{ord}_p(z - w),$$

hence (1) follows. ■

LEMMA 2. *If  $z \in \mathbb{Z}_p$ ,  $\text{ord}_p z \geq e_p - 1$  and*

$$F_n(z) = \sum_{i=1}^n (-1)^{i-1} \frac{z^i}{i},$$

*then*

$$\text{ord}_p(\log_p(1 + pz) - F_n(pz)) \geq (n + 1) \left(1 - \frac{2 - e_p}{p - 1}\right).$$

*Proof.* We have

$$\log_p(1 + pz) = F_n(pz) + \sum_{i=n+1}^{\infty} (-1)^{i-1} \frac{p^i}{i} z^i,$$

and the lemma follows from the estimate, valid for  $i \geq n + 1$ ,

$$\text{ord}_p \frac{p^i z^i}{i} > ie_p - \frac{i}{p - 1} \geq (n + 1) \left(1 - \frac{2 - e_p}{p - 1}\right). \quad \blacksquare$$

LEMMA 3. *For all integers  $a, b, c, d, e, f, p$  such that  $p \nmid ac$  and every non-negative integer  $\alpha$ , there exists an integer  $g$  such that if  $n \geq \alpha$  and*

$$n \equiv f \pmod{(p - 1)}, \quad n \equiv g \pmod{p^\alpha},$$

*then*

$$(2) \quad (an + b)c^n - de^n \equiv 0 \pmod{p^\alpha}.$$

*Proof.* If  $p | e$ , we take  $g$  such that  $ag + b \equiv 0 \pmod{p^\alpha}$ . If  $p \nmid e$ , let  $d = p^\gamma d_1$ , where  $d_1 \in \mathbb{Z}$ ,  $p \nmid d_1$ . If  $p = 2$  and  $\alpha = 1$ , we take  $g = d - b$ , thus for  $p = 2$  we assume  $\alpha \geq 2$ . Set

$$f_p = \begin{cases} d - b & \text{if } p = 2, 2 \nmid e, \\ f & \text{otherwise,} \end{cases}$$

and let  $h$  be an integer such that  $(ah + b)c^{f_p} \equiv de^{f_p} \pmod{p^\alpha}$ . We have  $h \equiv f_2 \pmod{2}$  if  $p = 2, 2 \nmid e$ . Taking  $n = h + p^{\gamma+e_p}z$ ,  $z \in \mathbb{Z}_p$ , by Lemma 1 we obtain

$$(3) \quad \begin{aligned} & \text{ord}_p((an + b)c^{f_p}c^{n-f_p} - de^{f_p}e^{n-f_p}) \\ & \geq \gamma + \min \left\{ \alpha - \gamma, \text{ord}_p \left( 1 + p^{e_p}ac^{f_p}d_1^{-1}e^{-f_p}z - \left(\frac{e}{c}\right)^{n-f_p} \right) \right\} \\ & = \gamma + \min \left\{ \alpha - \gamma, \text{ord}_p \left( \log_p(1 + p^{e_p}ac^{f_p}d_1^{-1}e^{-f_p}z) - \frac{n - f_p}{p^{e_p-1}(p - 1)} \beta \right) \right\}, \end{aligned}$$

where

$$\beta = \log_p \frac{e^{p^{e_p-1}(p-1)}}{c^{p^{e_p-1}(p-1)}}, \quad \text{ord}_p \beta \geq 2e_p - 1.$$

By Lemma 2,

$$(4) \quad \text{ord}_p \left( \log_p \left( 1 + p^{e_p} a c^{f_p} d_1^{-1} e^{-f_p z} \right) - \frac{h + p^{\gamma+e_p} z - f_p}{p^{e_p-1}(p-1)} \beta \right) \\ \geq \min \left\{ \alpha, \text{ord}_p \left( F_{\alpha_1} (p^{e_p} a c^{f_p} d_1^{-1} e^{-f_p z}) - \frac{h + p^{\gamma+e_p} z - f_p}{p^{e_p-1}(p-1)} \beta \right) \right\},$$

where

$$\alpha_1 = \left\lfloor \frac{\alpha}{1 - \frac{2-e_p}{p-1}} \right\rfloor.$$

We now apply Hensel's lemma to the polynomial

$$\mathcal{G}(z) = \frac{1}{p^{e_p}} F_{\alpha_1} (p^{e_p} a c^{f_p} d_1^{-1} e^{-f_p z}) - \frac{h + p^{\gamma+e_p} z - f_p}{p^{2e_p-1}(p-1)} \beta.$$

We have

$$\mathcal{G}'(z) \equiv a c^{f_p} d_1^{-1} e^{-f_p} - \frac{p^\gamma}{p-1} \cdot \frac{\beta}{p^{e_p-1}} \equiv a c^{f_p} d_1^{-1} e^{-f_p} \not\equiv 0 \pmod{p}.$$

There exists  $z_0 \in \mathbb{Z}_p$  such that  $\mathcal{G}(0) - z_0 \mathcal{G}'(0) = 0$ . Then  $\mathcal{G}(z_0) \equiv 0 \pmod{p}$ . Thus there exists  $z_1 \in \mathbb{Z}_p$  such that

$$F_{\alpha_1} (p^{e_p} a c^{f_p} d_1^{-1} e^{f_p z_1}) - \frac{h + p^{\gamma+e_p} z_1 - f_p}{p^{e_p-1}(p-1)} \beta = 0,$$

and taking for  $g$  the residue of  $h + p^{\gamma+e_p} z_1 \pmod{p^\alpha}$  we obtain (2) from (3) and (4). Note that for  $p \nmid ce$ , (2) depends only on the residue of  $n \pmod{p^\alpha(p-1)}$ .

**LEMMA 4.** *If  $a, b, c, d, e, m$  are integers with  $m > 0$  and  $(m, ac) = 1$ , then there exist infinitely many positive integers  $n$  such that  $m \mid (an + b)c^n - de^n$ .*

*Proof.* We proceed by induction on  $\omega(m)$ , the number of distinct prime factors of  $m$ . If  $\omega(m) = 1$ , Lemma 4 is contained in Lemma 3.

Suppose now that the lemma is true for  $\omega(m) = k-1 \geq 1$ , that  $\omega(m) = k$  and that  $p$  is the greatest prime factor of  $m$ . Thus  $p > 2$ . Let  $\text{ord}_p m = \alpha$ ,  $mp^{-\alpha} = m_0$ . Since  $\omega(m_0) = k-1$ , by the inductive assumption there exist infinitely many positive integers  $n$  such that  $m_0 \mid (an + b)c^n - de^n$ . Let  $n_0 \geq \max\{m_0, \alpha\}$  be one of these. By Lemma 3 there exists an integer  $g$  such that if  $n \equiv n_0 \pmod{p-1}$ ,  $n \equiv g \pmod{p^\alpha}$ ,  $n \geq \alpha$ , then  $p^\alpha \mid (an + b)c^n - de^n$ . However, if  $n \equiv n_0 \pmod{[m_0, \varphi(m_0)]}$  and  $n \geq m_0$ , then  $m_0 \mid (an + b)c^n - de^n$ . The congruences  $n \equiv n_0 \pmod{[m_0, \varphi(m_0), p-1]}$  and  $n \equiv g \pmod{p^\alpha}$  are compatible, since  $p \nmid m_0 \varphi(m_0)(p-1)$ , thus there exist infinitely many

positive integers  $n$  satisfying both of them. For these  $n \geq \max\{m_0, \alpha\}$  we have  $m \mid (an + b)c^n - de^n$ . ■

**COROLLARY 1.** *For every positive integer  $m$  there exist infinitely many positive integers  $n$  such that  $m \mid n + 2^n$ .*

*Proof.* It suffices to take in Lemma 4:  $a = 1$ ,  $b = 0$ ,  $c = 1$ ,  $d = -1$ ,  $e = 2$ . ■

**COROLLARY 2.** *For every prime  $p$  there exist infinitely many positive integers  $n$  such that  $p \mid n + 2^{n+2^n}$ .*

*Proof.* It suffices to take for  $p = 2$ , arbitrary even  $n$ , and for  $p > 2$ ,  $n \equiv -1 \pmod{p}$ , and if  $p - 1 \mid n_0 + 2^{n_0}$ ,  $n_0 \geq \text{ord}_2(p - 1)$  ( $n_0$  exists by Corollary 1), then we take  $n \equiv n_0 \pmod{\left[p - 1, \varphi\left(\frac{p-1}{2^{\text{ord}_2(p-1)}}\right)\right]}$ . ■

**COROLLARY 3.** *For every odd  $m$  and every  $\varepsilon \in \{1, -1\}$  there exist infinitely many integers  $n$  such that  $m \mid 2^n n + \varepsilon$ .*

*Proof.* It suffices to take in Lemma 4:  $a = 1$ ,  $b = 0$ ,  $c = 2$ ,  $d = -\varepsilon$ ,  $e = 1$ . ■

*Proof of the Theorem.* A ternary integral recurrence sequence with the companion polynomial  $(x - c)^2(x - e)$  ( $c \neq e$ ) is

$$f_1(n)c^n - f_2(n)e^n,$$

where  $f_i$  are polynomials of degree at most  $2 - i$  ( $i = 1, 2$ ),  $f_i \in \mathbb{Q}(a, c)[z]$  (see [2, p. 33, Theorem C.1]). Since the companion polynomial is monic with integral coefficients,  $c$  and  $e$  are integers and  $f_i \in \mathbb{Q}[z]$  ( $i = 1, 2$ ). Since the recurrence sequence is not binary,  $\deg f_i = 2 - i$  ( $i = 1, 2$ ) and  $ace \neq 0$ . Let

$$f_1 = \frac{az + b}{D_0}, \quad f_2 = \frac{d}{D_0}, \quad \text{where } a, b, d, D_0 \in \mathbb{Z}, \quad D_0 > 0.$$

It is enough to take  $D = |ac|D_0$  and apply Lemma 4. ■

**Acknowledgments.** A. Paszkiewicz has verified using a computer that for  $m \leq 20000$  there exist positive integers  $n$  satisfying the condition in Corollary 1, and found for each  $m$  the least  $n$ . W. Bednarek asked in a letter about the truth of Corollary 2.

## References

- [1] A. Schinzel, *Abelian binomials, power residues and exponential congruences*, Acta Arith. 32 (1977), 245–274; Addendum, *ibid.* 36 (1980), 101–104; also *Selecta*, Vol. 2, 939–970.
- [2] T. N. Shorey and R. Tijdeman, *Exponential Diophantine Equations*, Cambridge Tracts in Math. 87, Cambridge Univ. Press, Cambridge, 1997.
- [3] T. Skolem, *Anwendung exponentieller Kongruenzen zum Beweis der Unlösbarkeit gewisser diophantischer Gleichungen*, Vid. Akad. Avh. Oslo I, 1937, no. 12.

- [4] T. Skolem, *Diophantische Gleichungen*, Springer, 1938; reprint Chelsea, 1950.

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

*Received February 7, 2015;*  
*received in final form June 12, 2015*

(8011)

