BULLETIN OF THE POLISH
ACADEMY OF SCIENCES
MATHEMATICS
Vol. 58, No. 2, 2010

Büchi Sequences in Local Fields and Local Rings

by

Jerzy BROWKIN

Presented by Jerzy KACZOROWSKI

Summary. We prove that there exist infinite Büchi sequences in some local rings and local fields, with the exception of the ring $\mathbb{Z}_p$ of p-adic integers. In $\mathbb{Z}_p$ there are only finite but arbitrarily long Büchi sequences.

1. Introduction. A *Büchi sequence* of length M in a commutative ring A with unit is a solution $a_1, , \ldots, a_M \in A$ of the system of equations

$$x_{n+2}^2 - 2x_{n+1}^2 + x_n^2 = 2, \quad 1 \le n < M-1. \tag{1}$$

Here $3 \le M \le \infty$.

For every $a \in A$ and $\varepsilon_n \in \{-1, 1\}$, $1 \le n \le M$, the sequence

$$(\varepsilon_1(a+1), \varepsilon_2(a+2), \ldots, \varepsilon_M(a+M))$$

satisfies (1). We call it the *trivial Büchi sequence.*

Büchi's problem for a ring A is the following:

$\mathbf{B}^2(A)$: Does there exist a positive integer $M \ge 3$ such that every Büchi sequence of length M in the ring A is trivial?

The Büchi problem $\mathbf{B}^2(\mathbb{Z})$ is related to Hilbert's Tenth Problem (see [3]).

Büchi conjectured that every Büchi sequence of length 5 in $\mathbb{Z}$ is trivial, but this is still an open question.

In [1] an example is given of a nontrivial infinite Büchi sequence in the field $\mathbb{R}$ of real numbers (more precisely, in the ring of real algebraic integers). Namely, the sequence $a_n := \sqrt{n^2+1}$, $n \in \mathbb{N}$, is such an example, which can be easily verified. Here 1 can be replaced by any positive real algebraic integer. Moreover, the authors write, "We 'suspect' that $\mathbf{B}^2(\mathbb{Z}_p)$ has a negative answer as well."

2010 *Mathematics Subject Classification*: Primary 11B83; Secondary 11Sxx.
Key words and phrases: Büchi sequence, local rings, local fields.

DOI: 10.4064/ba58-2-2

They distinguish two kinds of rings in which Büchi problem has a negative answer:

Type 1: Rings for which there exists an infinite Büchi sequence.
Type 2: Rings for which there exist nontrivial Büchi sequences of any length, but there is no infinite one.

They give examples of rings of type 1 and they expect that there are also rings of type 2.

In the present paper we prove some results on the existence, respectively nonexistence, of nontrivial infinite Büchi sequences in some local fields and local rings. In particular we prove that $\mathbf{B}^2(\mathbb{Z}_p)$ has a negative answer, and the ring $\mathbb{Z}_p$ is of type 2.

2. The field $\mathbb{Q}_p$ of p-adic numbers and the ring $\mathbb{Z}_p$ of p-adic integers. First we investigate the existence of nontrivial infinite Büchi sequences in $\mathbb{Q}_p$ and in $\mathbb{Z}_p$. Next we generalize the results to more general local fields and local rings.

The case of the field of p-adic numbers is easy, as the following theorem shows.

THEOREM 1. *In the field $\mathbb{Q}_p$ there are nontrivial infinite Büchi sequences, e.g.*

$$\begin{aligned} a_n &:= \sqrt{n^2+p^{-2}}, \quad n\in\mathbb{N}, \quad \text{for } p>2,\\ a_n &:= \sqrt{n^2+2^{-4}}, \quad n\in\mathbb{N}, \quad \text{for } p=2. \end{aligned} \tag{2}$$

Proof. It is easy to verify that these sequences satisfy (1), and are nontrivial. It remains to prove that $a_n \in \mathbb{Q}_p$ for $n \in \mathbb{N}$.

For p odd we have

$$n^2+p^{-2} = (1+p^2n^2)/p^2$$

and $1+p^2n^2$ is a square in $\mathbb{Z}_p$, since every $a \in \mathbb{Z}_p$ satisfying $a \equiv 1 \pmod p$ is a square in $\mathbb{Z}_p$, by Hensel's lemma. Consequently, $a_n \in \mathbb{Q}_p$.

If $p=2$ we proceed similarly:

$$n^2+2^{-4} = (1+2^4n^2)/2^4,$$

and $1+2^4n^2$ is a square in $\mathbb{Z}_2$, since every $a \in \mathbb{Z}_2$ such that $a \equiv 1 \pmod 8$ is a square in $\mathbb{Z}_2$. Consequently, $a_n \in \mathbb{Q}_2$. ∎

REMARK 1. In the first formula of (2) the summand p^{-2} can be replaced by any element of $\mathbb{Q}_p$ which has even negative valuation. Similarly, in the second formula of (2) the summand 2^{-4} can be replaced by any element of $\mathbb{Q}_2$ which has an even valuation less than -2.

COROLLARY 1. *In every field F containing $\mathbb{Q}_p \cap \overline{\mathbb{Q}}$ there are nontrivial infinite Büchi sequences.*

Proof. The numbers a_n defined in Theorem 1 are algebraic over $\mathbb{Q}$, therefore they belong to the field F. ∎

Remark 2. Theorem 1 implies that the system (1) has a nontrivial solution everywhere locally. We do not know whether it has a nontrivial global solution, even a solution in $\mathbb{Q}$ for $M \geq 7$.

The numbers a_n defined in (2) are not p-adic integers. The next theorem shows that there are no p-adic integers with this property.

Theorem 2. *There is no nontrivial infinite Büchi sequence in the ring $\mathbb{Z}_p$ of p-adic integers.*

Proof. Assume that $(a_n)_{n\geq 1}$ is an infinite Büchi sequence with $a_n \in \mathbb{Z}_p$. Then, by definition,

$$a_{n+2}^2 = 2a_{n+1}^2 - a_n^2 + 2 \quad \text{for } n \geq 1.$$

It follows by induction that

$$a_n^2 = n^2 + (a_2^2 - a_1^2 - 3)n + (2a_1^2 - a_2^2 + 2) \quad \text{for } n \geq 1.$$

Consequently,

$$a_n^2 = \big(n + \tfrac{1}{2}(a_2^2 - a_1^2 - 3)\big)^2 + \big((2a_1^2 - a_2^2 + 2) - \tfrac{1}{4}(a_2^2 - a_1^2 - 3)^2\big). \tag{3}$$

We claim that $\frac{1}{2}(a_2^2 - a_1^2 - 3) \in \mathbb{Z}_p$. For $p > 2$ this is clear since 2 is invertible in $\mathbb{Z}_p$.

For $p = 2$ it is sufficient to prove that $2 \nmid a_2 - a_1$. Suppose that $2 \mid a_2 - a_1$. Then $4 \mid a_2^2 - a_1^2$, and from

$$a_3^2 = 2a_2^2 - a_1^2 + 2$$

we conclude that $a_3^2 \equiv a_2^2 + 2 \pmod 4$. This is impossible. ∎

To prove the theorem, in view of (3), it is sufficient to prove the following lemma.

Lemma 1. *Let p be a prime and let $a, b \in \mathbb{Z}_p$. Suppose that for every $n \geq 1$,*

$$f(n) := (n + a)^2 + b \tag{4}$$

is a square in $\mathbb{Z}_p$. Then $b = 0$.

Proof. (i) Suppose that p is odd, and let $g \in \mathbb{N}$ be a fixed primitive root modulo p.

Nonzero squares in $\mathbb{Z}_p$ are of the form

$$p^{2k} g^{2l}(1 + pc), \quad \text{where} \quad k \geq 0,\ l \geq 0,\ c \in \mathbb{Z}_p.$$

Hence the set of nonzero squares is closed (and open) in $\mathbb{Z}_p \setminus \{0\}$.

The set $\mathbb{N}$ of positive integers is dense in $\mathbb{Z}_p$, therefore for every $a \in \mathbb{Z}_p$ the set $\mathbb{N} + a := \{n + a : n \in \mathbb{N}\}$ is also dense in $\mathbb{Z}_p$.

If b is not a square, then for every $n+a$ sufficiently close to zero, $(n+a)^2+b$ is not a square, since the set of squares is closed.

This is a contradiction, since $f(n) = (n+a)^2 + b$ is a square for every $n \in \mathbb{N}$.

If b is a nonzero square, then

$$b = p^{2k} g^{2l}(1+pc)$$

for some $k \geq 0,\ l \geq 0,\ c \in \mathbb{Z}_p$.

It is well known that every nondegenerate quadratic form in two variables over a finite field represents all elements of the field (see e.g. [2, Theorem 1.2, p. 111 and Lemma 2.3, p. 116]).

In particular the form $x_1^2 + x_2^2$ represents the element g. Thus for some $\alpha, \beta \in \mathbb{Z}$ we have $g^{2\alpha} + g^{2\beta} \equiv g \pmod{p}$. Multiplying by $g^{2l-2\alpha}$ we get

$$g^{2l} + g^{2m} \equiv g^{2r+1} \pmod{p},$$

where $m = \beta - \alpha + l$, $r = l - \alpha$.

Now we choose $n \in \mathbb{N}$ such that $n + a = p^k g^m (1 + pc_1)$, where $c_1 \in \mathbb{Z}_p$, which is possible in view of the density of the set $\mathbb{N} + a$. Then

$$(n+a)^2 = p^{2k} g^{2m}(1+pc_2), \qquad c_2 \in \mathbb{Z}_p.$$

Consequently,

$$\begin{aligned} f(n) &= (n+a)^2 + b = p^{2k} g^{2m}(1+pc_2) + p^{2k} g^{2l}(1+pc) \\ &= p^{2k}(g^{2m} + g^{2l} + pc_3) = p^{2k} g^{2r+1}(1+pc_4) \end{aligned}$$

for some $c_3, c_4 \in \mathbb{Z}_p$. Thus $f(n)$ is not a square. We get a contradiction, so $b = 0$.

(ii) Now let $p = 2$. Nonzero squares in $\mathbb{Z}_2$ are of the form

$$2^{2k}(1+8c_1), \quad \text{where} \quad c_1 \in \mathbb{Z}_2. \tag{5}$$

The proof in this case is analogous, with the following change.

If $b = 2^{2k}(1+8c)$, then we choose $n+a$ of the form

$$n + a = 2^{k+1}(1+8c_1), \quad \text{where} \quad c_1 \in \mathbb{Z}_2.$$

Then

$$f(n) = (n+a)^2 + b = 2^{2k}(4+8c_2) + 2^{2k}(1+8c) = 2^{2k}(5+8c_3)$$

is not of the form (5).

Consequently, $f(n)$ is not a square in $\mathbb{Z}_2$. We get a contradiction, which implies that $b = 0$. ∎

THEOREM 3. *In the ring $\mathbb{Z}_p$ of p-adic integers there are arbitrarily long finite nontrivial Büchi sequences.*

Proof. For a fixed $k \geq 1$ let

$$a_n := \sqrt{n^2 + p^{2k+1}}.$$

For $n < p^k$ we have $v_p(n) < k$, hence $v_p(n^2) \le 2k-2$. Therefore

$$n^2 + p^{2k+1} = n^2(1 + p^3 \cdot p^{2k-2}/n^2)$$

is a square in $\mathbb{Z}_p$.

Thus $(a_1, \dots, a_M)$, where $M = p^k - 1$, is a nontrivial Büchi sequence of length $p^k - 1$ in $\mathbb{Z}_p$. Since $k = 1, 2, \dots$ we get examples of arbitrarily long nontrivial Büchi sequences. ∎

REMARK 3. 1. For $n = p^{k+1}$ the number $n^2 + p^{2k+1}$ is not a square in $\mathbb{Z}_p$, since $v_p(n^2 + p^{2k+1}) = 2k+1$ is odd. Therefore $a_n \notin \mathbb{Z}_p$.

2. From Theorems 2 and 3 it follows that in $\mathbb{Z}_p$ there are arbitrarily long finite nontrivial Büchi sequences, but there are no such infinite sequences. Therefore $\mathbb{Z}_p$ is an example of a ring of type 2.

3. More general local rings. Let F be a field complete with respect to a discrete valuation and let $\mathcal{O}_F$ be its ring of integers. Denote by π a generator of the maximal ideal of $\mathcal{O}_F$, and by v_π the corresponding valuation.

We shall use the following refinement of the Hensel lemma.

LEMMA 2 ([4, p. 76]). *Let $h \in \mathcal{O}_F[x]$ be a monic polynomial and let $h(u) \equiv 0 \pmod{\pi}$ for some $u \in \mathcal{O}_F$. Assume that*

$$v_\pi\left(\frac{h(u)}{h'(u)^2}\right) > 0. \tag{6}$$

Then there is $w \in \mathcal{O}_F$ such that $w \equiv u \pmod{\pi}$ and $h(w) = 0$. In other words, u can be refined to a root of $h(x)$ in $\mathcal{O}_F$.

COROLLARY 2. *Assume that the residue characteristic of F is 2. Let e be the ramification index of F over $\mathbb{Q}_2$. If $u \in \mathcal{O}_F$ satisfies $u \equiv 1 \pmod{\pi^{2e+1}}$, then u is a square in $\mathcal{O}_F$.*

Proof. Let $h(x) = x^2 - u$. Then $v_\pi(h(u)) = v_\pi(u-1) \ge 2e+1$ and $v_\pi(h'(u)^2) = v_\pi((2u)^2) = 2e$. Consequently, (6) holds. Then, by Lemma 2, u can be refined to a root $w \in \mathcal{O}_F$ of $h(x)$. Hence $u = w^2$ is a square in $\mathcal{O}_F$. ∎

THEOREM 4. *If F is a finite ramified extension of the field $\mathbb{Q}_p$, and $\mathcal{O}_F$ its ring of integers, then in $\mathcal{O}_F$ there are infinite nontrivial Büchi sequences.*

Proof. (i) Assume that p is odd. Let π be a generator of the maximal ideal of $\mathcal{O}_F$, and denote by v_π the corresponding valuation in F. We have $v_\pi(p) = e > 1$, where e is the ramification index of F over $\mathbb{Q}_p$. Then $e \mid v_\pi(n)$ for every $n \in \mathbb{N}$.

The sequence $a_n := \sqrt{n^2 + \pi^2}$, $n \in \mathbb{N}$, is a nontrivial infinite Büchi sequence, which is easy to verify.

It remains to prove that $a_n \in \mathcal{O}_F$, or equivalently that $n^2 + \pi^2$ is a square in $\mathcal{O}_F$ for $n \in \mathbb{N}$.

If $v_\pi(n) = 0$, then

$$n^2 + \pi^2 = n^2(1 + (\pi/n)^2) \quad \text{and} \quad v_\pi(\pi/n) = v_\pi(\pi) = 1 > 0.$$

Hence $n^2 + \pi^2$ is a square in $\mathcal{O}_F$.

If $v_\pi(n) > 0$, then $v_\pi(n) \geq e$, and

$$n^2 + \pi^2 = \pi^2(1 + (n/\pi)^2), \quad \text{where} \quad v_\pi(n/\pi) \geq e - 1 > 0.$$

Consequently, $n^2 + \pi^2$ is a square in $\mathcal{O}_F$.

(ii) Let $p = 2$. We shall prove that

$$f(n) := (n + \pi)^2 + \pi^{2e+3}$$

is a square in $\mathcal{O}_F$ for every $n \in \mathbb{N}$.

If n is odd, then $v(n + \pi) = 0$. Hence

$$f(n) = (n + \pi)^2 \left(1 + \frac{\pi^{2e+3}}{(n + \pi)^2}\right),$$

and $1 + \pi^{2e+3}/(n + \pi)^2$ is a square in $\mathcal{O}_F$, by Corollary 2.

If n is even, then $n = \pi^e n'$ for some $n' \in \mathcal{O}_F$, since $2\mathcal{O}_F = \pi^e \mathcal{O}_F$. We have $v(n + \pi) = v(\pi^e n' + \pi) = 1$, since $e > 1$.

Consequently,

$$f(n) = (n + \pi)^2 \left(1 + \frac{\pi^{2e+1}}{(\pi^{e-1} n' + 1)^2}\right),$$

and $1 + \pi^{2e+1}/(\pi^{e-1} n' + 1)^2$ is a square in $\mathcal{O}_F$, by Corollary 2. ∎

THEOREM 5. *Let F be a finite unramified extension of $\mathbb{Q}_p$ of degree > 1, and let $\mathcal{O}_F$ be the ring of integers of F. Then in $\mathcal{O}_F$ there are infinite nontrivial Büchi sequences.*

Proof. It is sufficient to find elements $a, b \in \mathcal{O}_F$, $b \neq 0$, such that

$$f(n) := (n + a)^2 + b$$

is a square in $\mathcal{O}_F$ for every $n \in \mathbb{N}$.

(i) Let p be an odd prime. Since F is an unramified extension of $\mathbb{Q}_p$, distinct from $\mathbb{Q}_p$, there is a canonical surjective homomorphism $\nu : \mathcal{O}_F \to \mathbb{F}_q$, where $\mathbb{F}_q$ is the residue field of F. Then $(\mathbb{F}_q : \mathbb{F}_p) = (F : \mathbb{Q}_p) > 1$, since F is unramified.

Therefore there is an element $a \in \mathcal{O}_F$ such that $\nu(a) \notin \mathbb{F}_p$. As $\nu(n) \in \mathbb{F}_p$ for every $n \in \mathbb{N}$, it follows that $\nu(n + a) \notin \mathbb{F}_p$. Then $\nu(n + a) \neq 0$, hence $v(n + a) = 0$.

Put $b := p$. Then $\nu(b) = 0$, hence

$$\nu(f(n)) = (\nu(n + a))^2 \in \mathbb{F}_q^{*2}.$$

By Hensel's lemma it follows that $f(n)$ is a square in $\mathcal{O}_F$ for every $n \in \mathbb{N}$.

(ii) Let $p = 2$. As above, we choose $a \in \mathcal{O}_F$ such that $\nu(a) \notin \mathbb{F}_2$. Then $v_2(n + a) = 0$ for every $n \in \mathbb{N}$.

We shall prove that $f(n) := (n+a)^2 + 8$ is a square in $\mathcal{O}_F$ for every $n \in \mathbb{N}$.

We have

$$f(n) = (n+a)^2\left(1 + \frac{8}{(n+a)^2}\right)$$

and $1 + 8/(n+a)^2$ is a square in $\mathcal{O}_F$, by Corollary 2. ∎

Let us observe that in fields and rings considered above there is a non-trivial infinite Büchi sequence iff the set $\mathbb{N}$ of positive integers is not dense in the field or the ring in question. This seems to be a general property.

We leave it to the reader as an amusing exercise to prove analogous results for general local fields and their rings of integers, namely for fields complete with respect to a discrete valuation with an arbitrary residue field, in particular in the case of equal characteristics.

References

[1] H. Pasten, T. Pheidas and X. Vidaux, *A survey on Büchi's problem: new presentations and open problems*, Proc. Hausdorff Institute of Mathematics, to appear.

[2] W. M. Schmidt, *Equations over Finite Fields: An Elementary Approach*, 2nd ed., Kendrick Press, 2004.

[3] P. Vojta, *Diagonal quadratic forms and Hilbert's Tenth Problem*, in: Contemp. Math. 270, Amer. Math. Soc., 2000, 261–274.

[4] E. Weiss, *Algebraic Number Theory*, McGraw-Hill, 1963.

Jerzy Browkin
Institute of Mathematics
Polish Academy of Sciences
Śniadeckich 8
00-956 Warszawa, Poland
E-mail: browkin@impan.pl

Received August 18, 2010 (7775)