Proyecciones Journal of Mathematics
Vol. 30, N^o 3, pp. 295-302, December 2011.
Universidad Católica del Norte
Antofagasta - Chile
DOI: 10.4067/S0716-09172011000300002

A NOTE ON BÜCHI'S PROBLEM FOR P-ADIC NUMBERS

MARIANELA CASTILLO
UNIVERSIDAD DE CONCEPCIÓN, CHILE
Received : March 2011. Accepted : September 2011

Abstract

We prove that for any prime p and any integer $k \geq 2$, there exist in the ring $\mathbf{Z}_p$ of p-adic integers arbitrarily long sequences whose sequence of k-th powers 1) has its k-th difference sequence equal to the constant sequence $(k!)$; and 2) is not a sequence of consecutive k-th powers. This shows that the analogue of Büchi's problem for higher powers has a negative answer over $\mathbf{Z}_p$. This result for $k = 2$ was recently obtained by J. Browkin.

MSC: 11D72, 11D88.

1. Introduction

Motivated by a mathematical logic problem, J.R. Büchi proposed the following problem in the early 1970's.

Problem 1.1 (Büchi's problem). $\mathbf{B}^2(\mathbf{Z})$. *Does there exist a positive integer M such that any sequence of M integer squares, with second difference constant equal to the constant sequence (2), is of the form $\big((x+n)^2\big)$, where $n = 1, \ldots, M$, for some integer x?*

Büchi's problem is open. In [6], Pheidas and Vidaux proposed a generalization of Büchi's problem to any unitary commutative ring and to higher powers.

Definition 1.2. *Let $k \geq 0$ be an integer. A sequence of elements of a unitary commutative ring A of characteristic 0 is called a k-Büchi sequence in A if the sequence of its k-th powers has k-th difference constant equal to $(k!)$. Every sequence whose sequence of k-th powers is of the form $\Big((x+n)^k\Big)$ for some x in A will be referred to as trivial k-Büchi sequence.*

Büchi's problem is generalized as follows (see [5] for a general survey).

Problem 1.3. $\mathbf{B}^k(A)$. *Let $k \geq 2$ be an integer and A a unitary commutative ring of characteristic 0. Does there exists an integer M such that every k-Büchi sequence in A of length M is trivial?*

We are interested in those rings for which Büchi's problem has a negative answer in a non-trivial way (intuitively, rings with not too many k-th powers). In [1], J. Browkin proved, in particular, that for $k = 2$, Büchi's problem for the ring of p-adic integers $\mathbf{Z}_p$ has a negative answer. This paper is an attempt to generalize to higher powers some of the results in Browkin's paper.

Theorem 1.4. *Let p be a prime number and $k \geq 2$ an integer.*

1. *For each $n \in \mathbf{Z}$, when $p > 2$ the quantity $n^k + p^{-k}$ is a k-th power in $\mathbf{Q}_p$. Moreover, any sequence (a_n), $n \geq 1$, such that a_n has k-th power $n^k + p^{-k}$, is a non-trivial k-Büchi sequence of infinite length in $\mathbf{Q}_p$.*

2. *For each $n \in \mathbf{Z}$, the quantity $n^k + 2^{-(2+k)}$ is a k-th power in $\mathbf{Q}_2$. Moreover, any sequence (a_n), $n \geq 1$, such that a_n has k-th power $n^k + 2^{-(2+k)}$, is a non-trivial k-Büchi sequence of infinite length in $\mathbf{Q}_2$.*

3. *For each $m \in \mathbf{Z}$, the quantity $n^k + p^{mk+1}$ is a k-th power in $\mathbf{Z}_p$ when $n = 1, \dots, p^m - 1$. Moreover, if $p^m \geq k+2$, then any sequence (a_n), $n = 1, \dots, p^m - 1$, where a_n has k-th power $n^k + p^{mk+1}$, is a non-trivial k-Büchi sequence in $\mathbf{Z}_p$.*

In Section 2, we give a characterization of the set of k-th powers in $\mathbf{Z}_p$, for each k and p. Some of the results seem to be well-known, but we were not able to find a proper reference. In Section 3, we will prove Items 1, 2 and 3 of our theorem.

For references on p-adic arithmetic, see for example [3].

I want to thank J. Browkin, H. Pasten and C. Videla for their useful comments during the preparation of this work, which is part of my Master thesis under the supervision of X. Vidaux.

2. Powers in $\mathbf{Z}_p$ and in $\mathbf{Q}_p$

Fix an integer $k \geq 2$ for the whole section.

Lemma 2.1. *Let $n \geq 1$ be an integer and suppose that either $p \neq 2$ or $n \neq 1$. The following equality holds: $(1+p^n\mathbf{Z}_p)^p = 1 + p^{1+n}\mathbf{Z}_p$.*

Proof. We use the fact that the exponential function is a group isomorphism between the additive group $p^n\mathbf{Z}_p$ and the multiplicative group $1 + p^n\mathbf{Z}_p$ whenever n is strictly bigger than $\frac{1}{p-1}$ - see [4, p. 38, Thm 1.2]. Therefore we have

$$\log\left((1 + p^n\mathbf{Z}_p)^p\right) = p^{n+1}\mathbf{Z}_p = \log(1 + p^{1+n}\mathbf{Z}_p).$$

□

Lemma 2.2. *The following equality holds: $(1+2\mathbf{Z}_2)^2 = 1 + 8\mathbf{Z}_2$*

Proof. Given $c \in \mathbf{Z}_2$, we have

$$(1+2c)^2 = 1 + 4c + 4c^2 = 1 + 4(c + c^2).$$

Since the first terms of c and of c^2 are either both 1 or both a positive power of 2, the quantity $c + c^2 \in 2\mathbf{Z}_2$. Therefore we have

$$(1+2\mathbf{Z}_2)^2 \subseteq 1 + 8\mathbf{Z}_2.$$

Now, given $c \in \mathbf{Z}_p$, consider the funcion $f(x) = x^2 - (1+8c)$ and its derivative $f'(x) = 2x$. We have

$$f'(1) = 2 \equiv 0 \bmod 2 \not\equiv 0 \bmod 2^2 \quad \text{and} \quad f(1) = -8c \equiv 0 \bmod 2^3.$$

By Hensel's Lemma, there exists $a \in \mathbf{Z}_2$ such that $f(a) = 0$ and $a \equiv 1 \bmod 2^2$. So, in particular, a belongs to $1 + 2\mathbf{Z}_2$. $\square$

Lemma 2.3. *Let $n \geq 0$ be an integer and suppose that $p \neq 2$. The following equality holds:*

$$(1 + p\mathbf{Z}_p)^{p^n} = 1 + p^{1+n}\mathbf{Z}_p. \tag{2.1}$$

Proof. The proof is analogous to that of Lemma 2.1. $\square$

Lemma 2.4. *For $n \geq 1$, the following equality holds:*

$$(1 + 2\mathbf{Z}_2)^{2^n} = 1 + 2^{2+n}\mathbf{Z}_2. \tag{2.2}$$

Proof. We prove the lemma by induction on n. By Lemma 2.2, we have

$$(1+2\mathbf{Z}_2)^2 = 1 + 8\mathbf{Z}_2$$

and Equality 2.2 holds for $n = 1$.

Suppose that Equation 2.2 holds up to n and let us prove that it holds for $n+1$. Indeed, by induction hypothesis, we have

$$(1+2\mathbf{Z}_2)^{2^{1+n}} = \left(1 + 2^{2+n}\mathbf{Z}_2\right)^2 = 1 + 2^{3+n}\mathbf{Z}_2,$$

where the last equality comes from the fact that $2 + n \neq 1$ and we can therefore apply Lemma 2.1. $\square$

Corollary 2.5. *For all integers $k \geq 2$ and for p an odd prime, the following equalities hold: $(1+p\mathbf{Z}_p)^k = 1 + p^{1+}$ and $(1+2\mathbf{Z}_2)^k = 1 + 2^{2+\mathrm{ord}_2 k}\mathbf{Z}_2$.*

Proof. Write $k = p^{\mathrm{ord}_p k} r$, where p does not divide r. Since p does not divide r, the map $x \mapsto x^r$ defines an automorphism of the multiplicative group of one-units $1 + p\mathbf{Z}_p$ (see Hasse [2, Ch. 15, Section 2, p. 215-217]) - note that the existence of an r-th root comes immediately from Hensel's Lemma, hence the map $x \mapsto x^r$ is a surjective morphism. Indeed, Hasse defines a map

$$\begin{array}{ccc} 1 + p\mathbf{Z}_p & \longrightarrow & 1 + p\mathbf{Z}_p \\ x & \longmapsto & x^c \end{array}$$

for any $c \in \mathbf{Z}_p$ and shows that it is an homomorphism of groups. Since r is invertible in $\mathbf{Z}_p$, the above map with $c = \frac{1}{r}$ is the reciprocal of $x \mapsto x^r$, which, therefore, is injective.

For $p > 2$, Lemma 2.3 gives

$$(1 + p\mathbf{Z}_p)^k = ((1 + p\mathbf{Z}_p)^r)^{p^{\mathrm{ord}_p k}} = (1 + p\mathbf{Z}_p)^{p^{\mathrm{ord}_p k}} = 1 + p^{1+\mathrm{ord}_p k}\mathbf{Z}_p,$$

and for $p = 2$ we apply Lemma 2.4 and find

$$(1 + 2\mathbf{Z}_2)^k = ((1 + 2\mathbf{Z}_2)^r)^{2^{\mathrm{ord}_2 k}} = (1 + 2\mathbf{Z}_2)^{2^{\mathrm{ord}_2 k}} = 1 + 2^{2+\mathrm{ord}_2 k}\mathbf{Z}_2.$$

□

Notation 2.6. *1. Let ε be 1 if $p = 2$ and 0 if $p \neq 2$.*

2. We will denote by S_p^k the set of non-zero k-th powers in $\mathbf{Z}_p$.

Lemma 2.7. *Let $g \in \mathbf{N}$ be a fixed primitive root modulo p. We have $S_p^k = \left\{ p^{km} g^{k\ell}(1 + p^{\varepsilon+1+\mathrm{ord}_p k} c) \colon m \geq 0, \ell \geq 0, c \in \mathbf{Z}_p \right\}$*

Proof. Let α be a non-zero k-th power in $\mathbf{Z}_p$, i.e. there is an integer $m \geq 0$ and there exists $\beta \in \mathbf{Z}_p$ invertible such that

$$\alpha = p^{km}\beta^k.$$

Since $\beta \in \mathbf{Z}_p^\times$, there are integers $a_i \in \{0, 1, \ldots, p-1\}$ such that

$$\beta = a_0 + a_1 p + a_2 p^2 + \ldots$$

where $a_0 \neq 0$. Since the residue class modulo p of a_0 is not 0, it is generated by the residue class of g in $\mathbf{F}_p^\times$, so there exists an integer $\ell \geq 0$ and an integer z such that $a_0 = g^\ell + pz$. We have

$$\beta = g^\ell \left(1 + p \left(\frac{1}{g^\ell}(z + a_1 + a_2 p + a_3 p^2 + \ldots) \right) \right).$$

Write $c = \frac{1}{g^\ell}(z + a_1 + a_2 p + a_3 p^2 + \ldots)$. Since $\mathrm{ord}_p(c) \geq 0$, we conclude that, for all non-zero k-th power α, there are integers $m \geq 0$ and $\ell \geq 0$, and a p-adic integer c such that

$$\alpha = p^{km} g^{k\ell}(1 + pc)^k$$

On the other hand, for all $c \in \mathbf{Z}_p$, the quantity $p^{km} g^{k\ell}(1 + pc)^k$ is trivially a k-th power. Finally, by Corollary 2.5, we have

$$S_p^k = p^{km} g^{k\ell}(1 + p\mathbf{Z}_p)^k = p^{km} g^{k\ell}(1 + p^{\varepsilon+1+\mathrm{ord}_p k}\mathbf{Z}_p).$$

□

3. Büchi sequences in $\mathbf{Z}_p$ and $\mathbf{Q}_p$ for any power

Fix an integer $k \geq 2$. The notation $\sqrt[k]{x}$ will refer to any specific k-th root of x.

Lemma 3.1. *For any prime number p and for any non-zero $b \in \mathbf{Q}_p$, the sequence (a_n) defined by $a_n = \sqrt[k]{n^k - b}$, $\quad 1 \leq n \leq M$ is a non-trivial Büchi sequence over the algebraic closure of $\mathbf{Q}_p$, whenever $M \geq k$.*

Proof. If (a_n) is trivial then, by definition, there exists $x \in \bar{\mathbf{Q}}_p$ such that

$$n^k - b = (x + n)^k$$

for each $n \geq 1$. If $x = 0$ then trivially $b = 0$, and if x is non-zero then b is a polynomial in n of degree $k - 1 \geq 1$, which is impossible since the sequence has length greater than $k - 1$. □

Proof. [Proof of Item 1 of the main theorem] By Lemma 3.1 we need only prove that for each integer $n \in \mathbf{Z}$, the quantity $n^k + p^{-k} \in \mathbf{Q}_p$ is a k-th power in $\mathbf{Q}_p$, which is equivalent to prove that $p^k n^k + 1$ is a k-th power in $\mathbf{Z}_p$. For each k and p we have $k \geq 1 + \mathrm{ord}_p k$, hence the quantity $c = p^{k-1-\mathrm{ord}_p k} n^k$ is a p-adic integer and we deduce that

$$1 + p^k n^k = 1 + p^{1+\mathrm{ord}_p k}\left(p^{k-1-\mathrm{ord}_p k} n^k\right)$$

is a k-th power by Lemma 2.7. □

Proof. [Proof of Item 2 of the main theorem] Again, we prove that for each integer $n \in \mathbf{Z}$, the quantity $n^k + 2^{-(2+k)}$ is a k-th power in $\mathbf{Q}_2$, which is equivalent to prove that $2^{2+k}n^k + 1$ is a k-th power in $\mathbf{Z}_2$. Since for each k we have $k \geq \mathrm{ord}_2 k$, we deduce that $c = 2^{k-\mathrm{ord}_2 k} n^k$ is a p-adic integer and therefore

$$1 + 2^{2+k}n^k = 1 + 2^{2+\mathrm{ord}_2 k}\left(2^{k-\mathrm{ord}_2 k}n^k\right)$$

is a k-th power by Lemma 2.7. □

Proof. [Proof of Item 3 of the main theorem] Similarly, for every $m \geq 1$, we want to prove that the quantity $n^k + p^{km+1}$ is a k-th power in $\mathbf{Z}_p$ for $n = 1, \ldots, p^m - 1$. By Lemma 2.7, since

$$n^k + p^{km+1} = n^k\left(1 + p^{2+\mathrm{ord}_p k}\frac{p^{km-1-\mathrm{ord}_p k}}{n^k}\right)$$

we need only prove that the quantity

$$\frac{p^{km-1-\mathrm{ord}_p k}}{n^k}$$

is a p-adic integer. Since $n < p^m$, we have $\mathrm{ord}_p n \leq m - 1$, hence

$$\mathrm{ord}_p n^k \leq km - k \leq km - (1 + \mathrm{ord}_p k).$$

Finally we obtain

$$\mathrm{ord}_p\left(\frac{p^{km-1-\mathrm{ord}_p k}}{n^k}\right) = km - (1 + \mathrm{ord}_p k) - \mathrm{ord}_p n^k \geq 0.$$

□

Note that the sequence used for the above proof can not be extended to an infinite sequence. Actually, if $n = p^{m+1}$, then $\mathrm{ord}_p\left(n^k + p^{km+1}\right) = \min\left\{\mathrm{ord}_p\left(p^{km+k}\right), \mathrm{ord}_p\left(p^{km+1}\right)\right\} = km + 1$ which is not a multiple of k, therefore, $n^k + p^{km+1}$ is not a k-th power in $\mathbf{Z}_p$.

References

[1] J. Browkin, Büchi sequences in local fields and local rings, Bull. Polish Acad. Sci. Math. **58**, 109-115 (2010).

[2] H. Hasse, Number Theory, Springer (1980).

[3] N. Koblitz, P-adic Numbers, p-adic Analysis, and Zeta-Functions, Springer Graduate Texts in Mathematics, (1996).

[4] J. Neukirch, Class field theory, Springer Verlag, Grundlehren der mathematischen Wissenschaften **280**, A Series of Comprehensive Studies in Mathematics, (1986).

[5] H. Pasten, T. Pheidas and X. Vidaux, A survey on Büchi's problem: new presentations and open problems, Zapiski Nauchn. Sem. POMI **377**, pp. 111-140, (2010).

[6] T. Pheidas and X. Vidaux, Extensions of Büchi's problem: Questions of decidability for addition and n-th powers, Fundamenta Mathematicae **185**, pp. 171-194, (2005).

Marianela Castillo
Universidad de Concepción
Casilla 160-C
Concepción
e-mail : mcastillo@udec.cl