C. R. Acad. Sci. Paris, Ser. I 349 (2011) 947–952

Contents lists available at ScienceDirect

C. R. Acad. Sci. Paris, Ser. I

www.sciencedirect.com

Number Theory

Analytic functions over $\mathbb{Z}_p$ and p-regular sequences

Fonctions analytiques sur $\mathbb{Z}_p$ et suites p-régulières

Zhang Shu, Jia-Yan Yao

Department of Mathematics, Tsinghua University, 100084 Beijing, PR China

ARTICLE INFO

Article history:
Received 13 June 2011
Accepted after revision 1 August 2011
Available online 31 August 2011

Presented by Jean-Pierre Kahane

ABSTRACT

Let p be a prime number. In this work we characterize all the analytic functions $f:\mathbb{Z}_p\to\mathbb{C}_p$ without roots in $\mathbb{N}$ for which the sequence $(v_p(f(n)))_{n\geqslant 0}$ is p-regular. Then we apply our characterization to study quadratic linear recurrent sequences.

RÉSUMÉ

Soit p un nombre premier. Dans ce travail, nous caractérisons les fonctions analytiques $f:\mathbb{Z}_p\to\mathbb{C}_p$ sans zéros dans $\mathbb{N}$ pour lesquelles la suite $(v_p(f(n)))_{n\geqslant 0}$ est p-régulière. Ensuite nous appliquons notre caractérisation pour étudier les suites récurrentes linéaires quadratiques.

Version française abrégée

Soit p un nombre premier. Nous désignons par $\mathbb{Z}_p$ l'anneau des entiers p-adiques, et par $\mathbb{Q}_p$ le corps des fractions de $\mathbb{Z}_p$. Soit $\mathbb{C}_p$ le complété topologique d'une clôture algébrique fixée de $\mathbb{Q}_p$. Nous désignons par v_p la valuation p-adique sur $\mathbb{C}_p$ normalisée telle que $v_p(p)=1$, et par $|\cdot|_p$ la valeur absolue associée telle que $|z|_p=p^{-v_p(z)}$, pour tout $z\in\mathbb{C}_p$. Finalement nous rappelons qu'une suite $(u(n))_{n\geqslant 0}$ à valeurs dans $\mathbb{Q}$ est p-régulière si le $\mathbb{Z}$-module engendré par

$$\mathcal{N}_p(u)=\left\{\left(u\left(p^bn+a\right)\right)_{n\geqslant 0}\,\middle|\,b\geqslant 0,0\leqslant a<p^b\right\}$$

est de type fini. Pour savoir plus sur les suites régulières, voir J.-P. Allouche et J.O. Shallit [1,2] (voir aussi [3]).

Dans cette Note, nous allons démontrer le résultat suivant :

Théorème 2. *Soit $f:\mathbb{Z}_p\to\mathbb{C}_p$ une fonction analytique sans zéros dans $\mathbb{N}$. Alors la suite $(v_p(f(n)))_{n\geqslant 0}$ est p-régulière si et seulement si tous les zéros de f dans $\mathbb{Z}_p$ sont contenus dans $\mathbb{Q}$.*

En appliquant aux suites récurrentes linéaires quadratiques, nous aurons aussi le résultat suivant :

Théorème 3. *Soit $x=(x(n))_{n\geqslant 0}$ une suite dans $\mathbb{Q}_p\setminus\{0\}$ telle que pour tous les entiers $n\geqslant 0$, nous avons $x(n+2)=Ax(n+1)+Bx(n)$, où $A,B\in\mathbb{Q}_p\setminus\{0\}$ sont constants. Posons $v_p(x)=(v_p(x(n)))_{n\geqslant 0}$, et désignons par α_1,α_2 les racines de l'équation $X^2-AX-B=0$. Nous avons les classifications suivantes.*

E-mail addresses: shuzhang999@126.com (Z. Shu), jyyao@math.tsinghua.edu.cn (J.-Y. Yao).

1631-073X/$ – see front matter
doi:10.1016/j.crma.2011.08.001

Cas I : $\alpha_1 = \alpha_2$. Alors il existe $a, b \in \mathbb{Q}_p$ tel que $x(n) = (an+b)\alpha_1^n$ pour tous les entiers $n \geqslant 0$, et $v_p(x)$ n'est pas p-régulière si et seulement si $a \neq 0$ et $-b/a \in \mathbb{Z}_p \setminus \mathbb{Q}$.

Cas II : $\alpha_1 \neq \alpha_2$. Alors pour tous les entiers $n \geqslant 0$, nous avons $x(n) = a\alpha_1^n + b\alpha_2^n$. Nous avons besoin de distinguer trois cas encore.

Cas (1) : $ab = 0$. Alors $v_p(x)$ est p-régulière.

Cas (2) : $ab \neq 0$, et $|a|_p \neq |b|_p$ ou $|\alpha_1|_p \neq |\alpha_2|_p$. Alors $v_p(x)$ est p-régulière.

Cas (3) : $ab \neq 0$, $|a|_p = |b|_p$ et $|\alpha_1|_p = |\alpha_2|_p$. Posons $u = b/a$, $\gamma = \alpha_2/\alpha_1$, et $\ell = p^2 - 1$. Alors pour tous les entiers $0 \leqslant l < p^2\ell$, il existe une fonction analytique φ_l définie sur $\mathbb{Z}_p$ telle que pour tous les entiers $n \geqslant 0$, nous avons $\varphi_l(n) = 1 + u\gamma^{p^2\ell n+l}$. Dans ce cas $v_p(x)$ n'est pas p-régulière si et seulement s'il existe $\theta \in \mathbb{Z}_p \setminus \mathbb{Q}$ tel que $\varphi_l(\theta) = 0$ pour certain entier $0 \leqslant l < p^2\ell$.

1. Statements of main results

Fix p a prime number. We denote by $\mathbb{Z}_p$ the ring of p-adic integers, and by $\mathbb{Q}_p$ the field of fractions of $\mathbb{Z}_p$. Let $\mathbb{C}_p$ be the topological completion of a fixed algebraic closure of $\mathbb{Q}_p$. We denote by v_p the p-adic valuation over $\mathbb{C}_p$ normalized such that $v_p(p) = 1$, and by $|\cdot|_p$ the associated absolute value such that $|z|_p = p^{-v_p(z)}$, for all $z \in \mathbb{C}_p$. Then v_p takes values in $\mathbb{Q} \cup \{+\infty\}$.

The starting point of our present work is the following result of J.P. Bell [5] which solved an interesting problem put forward by J.-P. Allouche and J.O. Shallit in [1] (see also [3]):

Theorem 1. *Let $f \in \mathbb{Z}_p[X]$ be a polynomial which does not have any root in $\mathbb{N} = \{0, 1, \dots, \}$. Then the sequence $(v_p(f(n)))_{n\geqslant 0}$ is p-regular if and only if all the roots of f in $\mathbb{Z}_p$ are contained in $\mathbb{Q}$.*

Inspired and motivated by the above result, in this Note we shall show the following theorem, and then apply it to study quadratic linear recurrent sequences:

Theorem 2. *Let $f : \mathbb{Z}_p \to \mathbb{C}_p$ be an analytic function which does not have any root in $\mathbb{N}$. Then the sequence $(v_p(f(n)))_{n\geqslant 0}$ is p-regular if and only if all the roots of f in $\mathbb{Z}_p$ are contained in $\mathbb{Q}$.*

Recall that f is analytic on $\mathbb{Z}_p$ if and only if f can be expanded as a Taylor series at each point in $\mathbb{Z}_p$, and that a sequence $(u(n))_{n\geqslant 0}$ with values in $\mathbb{Q}$ is p-regular if the $\mathbb{Z}$-module generated by

$$\mathcal{N}_p(u) = \left\{ \left(u\left(p^b n + a\right)\right)_{n\geqslant 0} \,\middle|\, b \geqslant 0, 0 \leqslant a < p^b \right\}$$

is a finitely generated $\mathbb{Z}$-module. Recall also that for any integer $m \geqslant 1$, a sequence $(u(n))_{n\geqslant 0}$ is p-regular if and only if $(u(mn+l))_{n\geqslant 0}$ is p-regular for all integers $0 \leqslant l < m$. Finally recall that a p-regular sequence remains p-regular after changing a finite number of terms. For a more general definition and more details about regular sequences, see J.-P. Allouche and J.O. Shallit [1,2] (see also [3]).

As an application to quadratic linear recurrent sequences, we have the following classification:

Theorem 3. *Let $x = (x(n))_{n\geqslant 0}$ be a sequence in $\mathbb{Q}_p \setminus \{0\}$ such that for all integers $n \geqslant 0$, we have*

$$x(n+2) = Ax(n+1) + Bx(n),$$

where $A, B \in \mathbb{Q}_p \setminus \{0\}$ are constants. Set $v_p(x) = (v_p(x(n)))_{n\geqslant 0}$, and denote by α_1, α_2 the roots of the characteristic equation $X^2 - AX - B = 0$. We distinguish different situations below.

Case I: *$\alpha_1 = \alpha_2$. Then there exist $a, b \in \mathbb{Q}_p$ such that $x(n) = (an+b)\alpha_1^n$ for all integers $n \geqslant 0$, and $v_p(x)$ is not p-regular if and only if $a \neq 0$ and $-b/a \in \mathbb{Z}_p \setminus \mathbb{Q}$.*

Case II: *$\alpha_1 \neq \alpha_2$. Then $x(n) = a\alpha_1^n + b\alpha_2^n$, for all integers $n \geqslant 0$. We distinguish three cases again.*

Case (1): *$ab = 0$. Then $v_p(x)$ is p-regular.*

Case (2): *$ab \neq 0$, and $|a|_p \neq |b|_p$ or $|\alpha_1|_p \neq |\alpha_2|_p$. Then $v_p(x)$ is p-regular.*

Case (3): *$ab \neq 0$, $|a|_p = |b|_p$ and $|\alpha_1|_p = |\alpha_2|_p$. Set $u = b/a$, $\gamma = \alpha_2/\alpha_1$, and $\ell = p^2 - 1$. Then for all integers $0 \leqslant l < p^2\ell$, there exists an analytic function φ_l defined on $\mathbb{Z}_p$ such that for all integers $n \geqslant 0$, we have $\varphi_l(n) = 1 + u\gamma^{p^2\ell n+l}$. In this case $v_p(x)$ is not p-regular if and only if there exists $\theta \in \mathbb{Z}_p \setminus \mathbb{Q}$ such that $\varphi_l(\theta) = 0$ for some integer $0 \leqslant l < p^2\ell$.*

2. Proof of Theorem 2

For all $a \in \mathbb{Z}_p$ and all integers $k \geqslant 0$, put $B_k(a) = \{z \in \mathbb{Z}_p\colon\ |z - a|_p \leqslant p^{-k}\}$. We say that $f : B_k(a) \to \mathbb{C}_p$ is strictly analytic on $B_k(a)$ if there exists a sequence $(c_n)_{n\geqslant 0}$ in $\mathbb{C}_p$ such that

$$f(z)=\sum_{n=0}^{+\infty}c_n(z-a)^n,$$

and the disk of convergence contains $B_k(a)$. For more details on strictly analytic functions, see [4, p. 107].

Lemma. *If f is strictly analytic on $\mathbb{Z}_p$ and does not have any root in $\mathbb{Z}_p$, then $(v_p(f(n)))_{n\geqslant 0}$ is periodic.*

Proof. Suppose that f does not have any root in $\mathbb{Z}_p$. Since f is continuous, then we can find an integer $m\geqslant 1$ such that $f \pmod{p^m}$ does not have any root in $\mathbb{Z}/p^m\mathbb{Z}$. Hence for all $z\in\mathbb{Z}_p$, we have $v_p(f(z))<m$. Since the convergence of disk of f contains $\mathbb{Z}_p$, then for any $b\in\mathbb{Z}_p$, we have, by virtue of [4, p. 107],

$$f(b+1)=f(b)+\sum_{j=1}^{+\infty}\frac{f^{(j)}(b)}{j!},$$

and then $\lim_{j\to+\infty}v_p(f^{(j)}(b)/j!)=+\infty$. Thus there exists some $D(b)\in\mathbb{Z}$ such that $v_p(f^{(j)}(b)/j!)>D(b)$, for all $j\in\mathbb{N}$. Set $M(b)=|[(m-D(b))/m]|+1$. Then for all $\alpha\in\mathbb{Z}_p$ and for all integers $j\geqslant 1$, we obtain

$$v_p\left(\frac{f^{(j)}(b)}{j!}\left(\alpha p^{M(b)m}\right)^j\right)>D(b)+M(b)m>m.$$

Now that f is strictly analytic on $\mathbb{Z}_p$, thus for all $\alpha\in\mathbb{Z}_p$, we have

$$f\left(b+\alpha p^{M(b)m}\right)=f(b)+\sum_{j=1}^{+\infty}\frac{f^{(j)}(b)}{j!}\left(\alpha p^{M(b)m}\right)^j,$$

hence $v_p(f(b+\alpha p^{M(b)m}))=v_p(f(b))$, for we have $v_p(f(b))<m$. Set $B_b=B_{M(b)m}(b)$. Then $(B_b)_{b\in\mathbb{Z}_p}$ forms an open covering of $\mathbb{Z}_p$, and we can find $b_1,\dots,b_k\in\mathbb{Z}_p$ such that $(B_{b_j})_{1\leqslant j\leqslant k}$ covers $\mathbb{Z}_p$. Set

$$N=\max_{1\leqslant j\leqslant k}M(b_j)m.$$

For any $n\in\mathbb{N}$, we can find some integer j $(1\leqslant j\leqslant k)$ such that $n\in B_{b_j}$. Then $n+p^N\in B_{b_j}$, and thus

$$v_p\left(f(n)\right)=v_p\left(f(b_j)\right)=v_p\left(f\left(n+p^N\right)\right).$$

So the sequence $(v_p(f(n)))_{n\geqslant 0}$ is periodic. □

Now we are ready to prove Theorem 2.

Since f is analytic on $\mathbb{Z}_p$, then $\forall a\in\mathbb{Z}_p$, we can find an integer $k(a)\geqslant 1$ such that f is strictly analytic on $B_{k(a)}(a)$. Now that $\mathbb{Z}_p$ is compact, thus there exist $a_1,\dots,a_N\in\mathbb{Z}_p$ such that $\mathbb{Z}_p=\bigcup_{i=1}^N B_{k(a_i)}(a_i)$. Set $k=\max_{1\leqslant i\leqslant N}k(a_i)$. Then for any integer j $(0\leqslant j<p^k)$, there exists an integer i $(1\leqslant i\leqslant n)$ such that $B_k(j)\subseteq B_{k(a_i)}(a_i)$. Note that $(v_p(f(n)))_{n\geqslant 0}$ is p-regular if and only if $(v_p(f(p^kn+j)))_{n\geqslant 0}$ is p-regular for all integers j $(0\leqslant j<p^k)$, hence up to replacing the function $f(z)$ by $f(p^kz+j)$, we can suppose in the following that f is strictly analytic on $\mathbb{Z}_p$:

Necessity. By contradiction, assume that $(v_p(f(n)))_{n\geqslant 0}$ is p-regular and there exists some $\theta\in\mathbb{Z}_p\backslash\mathbb{Q}$ such that $f(\theta)=0$. Then we can find an integer $d\geqslant 1$ such that $f(z)=(z-\theta)^d g(z)$, where g is strictly analytic on $\mathbb{Z}_p$. Write $\theta=\sum_{i=0}^{+\infty}\alpha_i p^i$ $(0\leqslant \alpha_i<p)$, and for all integers $j\geqslant 1$, define

$$\theta_j=\sum_{i=0}^{j-1}\alpha_i p^i\quad\text{and}\quad\delta_j=\theta_j-\theta.$$

Note that g is strictly analytic on $\mathbb{Z}_p$, then as above, we can find $M\in\mathbb{Z}$ such that for all integers $i\geqslant 0$, we have $v_p(g^{(i)}(\theta)/i!)>M$. Fix $j=|[v_p(g(\theta))]-M|+2$. Then for all integers $n\geqslant 0$ and $i\geqslant 1$, we have

$$v_p\left(\left(\delta_j+p^jn\right)^i\frac{g^{(i)}(\theta)}{i}\right)>j+M>v_p\left(g(\theta)\right),$$

from which we deduce immediately

$$v_p\left(g\left(p^jn+\theta_j\right)\right)=v_p\left(g\left(\theta+\delta_j+p^jn\right)\right)=v_p\left(g(\theta)+\sum_{i=1}^{+\infty}\left(\delta_j+p^jn\right)^i\frac{g^{(i)}(\theta)}{i!}\right)=v_p\left(g(\theta)\right).$$

Consequently we obtain

$$v_p\big(f\big(p^j n+\theta_j\big)\big)=d v_p\big(p^j n+\theta_j-\theta\big)+v_p\big(g\big(p^j n+\theta_j\big)\big)=d\big(j+v_p\big(n+\delta_j p^{-j}\big)\big)+v_p\big(g(\theta)\big).$$

But $\delta_j p^{-j}\in\mathbb{Z}_p\backslash\mathbb{Q}$, thus $(v_p(n+\delta_j p^{-j}))_{n\geqslant 0}$ is not p-regular by Theorem 1. So $(v_p(f(p^j n+\theta_j)))_{n\geqslant 0}$ is not p-regular either. This is absurd!

Sufficiency. Suppose that $\{\alpha\in\mathbb{Z}_p \mid f(\alpha)=0\}\subseteq\mathbb{Q}$. Since $\mathbb{Z}_p$ is compact, f is strictly analytic on $\mathbb{Z}_p$ and does not have any root in $\mathbb{N}$, thus we can write $f(z)=h(z)\prod_{i=1}^{k}(z-\alpha_i)$, where $\alpha_i\in\mathbb{Z}_p\cap\mathbb{Q}$ $(1\leqslant i\leqslant k)$, and h is strictly analytic on $\mathbb{Z}_p$ and does not have any root in $\mathbb{Z}_p$. Then $(v_p(n-\alpha_i))_{n\geqslant 0}$ is p-regular by Theorem 1, and $(v_p(h(n)))_{n\geqslant 0}$ is periodic by our lemma. So $(v_p(f(n)))_{n\geqslant 0}$ is p-regular.

3. Proof of Theorem 3

We shall show the result by distinguishing different situations.

Case I: $\alpha_1=\alpha_2$. Then there exist $a,b\in\mathbb{Q}_p$ such that $x(n)=(an+b)\alpha_1^n$ for all integers $n\geqslant 0$. Thus $v_p(x(n))=v_p(an+b)+n v_p(\alpha)$. But $(n v_p(\alpha))_{n\geqslant 0}$ is p-regular, so by Theorem 1, we know that $v_p(x)$ is not p-regular if and only if $a\neq 0$ and $-b/a\in\mathbb{Z}_p\setminus\mathbb{Q}$.

Case II: $\alpha_1\neq\alpha_2$. We need distinguish three cases again.

Case (1): $a=0$ or $b=0$. Then for all integers $n\geqslant 0$, we have

$$v_p\big(x(n)\big)=v_p(b)+n v_p(\alpha_2)\quad\text{or}\quad v_p(a)+n v_p(\alpha_1).$$

So $v_p(x)$ is p-regular.

Case (2): $ab\neq 0$. If $|\alpha_1|_p\neq|\alpha_2|_p$, then by symmetry we can suppose $|\alpha_1|_p>|\alpha_2|_p$. Hence for all integers $n\geqslant 0$ large enough, we have

$$v_p\big(x(n)\big)=n v_p(\alpha_1)+v_p\left(a+b\left(\frac{\alpha_2}{\alpha_1}\right)^n\right)=n v_p(\alpha_1)+v_p(a).$$

So $v_p(x)$ is p-regular, for a p-regular sequence remains p-regular after changing a finite number of terms.

If $|\alpha_1|_p=|\alpha_2|_p$ and $|a|_p\neq|b|_p$, we can also assume $|a|_p>|b|_p$, and then for all integers $n\geqslant 0$,

$$v_p\big(x(n)\big)=n v_p(\alpha_1)+v_p(a)+v_p\left(1+\frac{b}{a}\left(\frac{\alpha_2}{\alpha_1}\right)^n\right)=n v_p(\alpha_1)+v_p(a).$$

Thus $v_p(x)$ is p-regular again.

Case (3): $ab\neq 0$, $|a|_p=|b|_p$ and $|\alpha_1|_p=|\alpha_2|_p$. Then for all integers $n\geqslant 0$, we have

$$v_p\big(x(n)\big)=v_p(a)+n v_p(\alpha_1)+v_p\big(1+u\gamma^n\big).$$

But $(v_p(a)+n v_p(\alpha_1))_{n\geqslant 0}$ is p-regular, hence we need only consider $(v_p(1+u\gamma^n))_{n\geqslant 0}$.

Let O be the ring of integers of $\mathbb{Q}_p[\sqrt{A^2+4B}\,]$, and π a prime element of O. Now that $|\gamma|_p=1$, we can write uniquely $\gamma=u_0(1+\pi\gamma_0)$, with $u_0\in O$ a root of unity (thus $u_0^{\ell}=1$), and $\gamma_0\in O$ (see [7, p. 19]). Then for all integers $n\geqslant 0$ and $0\leqslant l<p^2\ell$, we have

$$1+u\gamma^{p^2\ell n+l}=1+u\gamma^l(1+\pi\gamma_0)^{p^2\ell n}=1+u\gamma^l\big(1+p\pi\gamma_1+(\pi\gamma_0)^{p^2}\big)^{\ell n},$$

with $\gamma_1\in O$. However $v_p((\pi\gamma_0)^{p^2})\geqslant p^2\cdot v_p(\pi)\geqslant 4\cdot\frac{1}{2}=2$ and $v_p(p\pi\gamma_1)\geqslant 1+v_p(\pi)>1$, thus

$$v_p\big(p\pi\gamma_1+(\pi\gamma_0)^p\big)>1\geqslant\frac{1}{p-1}.$$

With the help of logarithm and exponential (see [4, p. 102] or [7, p. 70]), we can define, for all $z\in\mathbb{Z}_p$,

$$\varphi_l(z)=1+u\gamma^l\exp\big(\ell z\log\big(1+p\pi\gamma_1+(\pi\gamma_0)^{p^2}\big)\big).$$

Then φ_l is analytic on $\mathbb{Z}_p$ and for all integers $n\geqslant 0$, we have $\varphi_l(n)=1+u\gamma^{p^2\ell n+l}$.

To conclude, it suffices to note that $v_p(x)$ is p-regular if and only if $v_p(x(p^2\ell n+l))_{n\geqslant 0}$ is p-regular for all integers $0\leqslant l<p^2\ell$, and then apply Theorem 2. □

Remarks. (1) Using the same arguments as above, we can also show that Theorem 3 holds for quadratic linear recurrent sequences with values in an algebraic extension of $\mathbb{Q}_p$.

(2) Let $d \geqslant 2$ be an integer and $x = (x(n))_{n \geqslant 0}$ a sequence in $\mathbb{Q}$ such that for all integers $n \geqslant 0$, holds

$$x(n+d) = \sum_{j=0}^{d-1} a_j x(n+j),$$

where $a_j \in \mathbb{Q}$ $(0 \leqslant j \leqslant d-1)$. Let α_i $(1 \leqslant i \leqslant k)$ be the nonzero roots of the characteristic polynomial $X^d - \sum_{j=0}^{d-1} a_j X^j$. Except for a finite number of premier numbers p, we have $|\alpha_i|_p = 1$ $(1 \leqslant i \leqslant k)$, and then we can obtain a similar characterization as in the Case II (3) of Theorem 3.

4. Some corollaries

Conditions in the Case II (3) of Theorem 3 are difficult to check. Below we give some easy criteria.

Theorem 4. *Let $x = (x(n))_{n \geqslant 0}$ be a sequence in $\mathbb{Q}_p \setminus \{0\}$ such that for all integers $n \geqslant 0$, we have*

$$x(n+2) = Ax(n+1) + Bx(n),$$

where $A, B \in \mathbb{Q}_p \setminus \{0\}$ are constants. If $x(1) = Ax(0)$, then $v_p(x)$ is p-regular.

Proof. We shall follow the classification in Theorem 3:

Case I: $\alpha_1 = \alpha_2$. Then $\alpha_1 = A/2$. But $x(1) = Ax(0)$, so $a = b$, and $v_p(x)$ is p-regular by Theorem 3.

Case II: $\alpha_1 \neq \alpha_2$. Then from the fact $x(1) = Ax(0)$, we obtain

$$a = \frac{\alpha_2 x(0) - x(1)}{\alpha_2 - \alpha_1} = \frac{-\alpha_1 x(0)}{\alpha_2 - \alpha_1} \quad \text{and} \quad b = \frac{x(1) - \alpha_1 x(0)}{\alpha_2 - \alpha_1} = \frac{\alpha_2 x(0)}{\alpha_2 - \alpha_1}.$$

Set $c = x(0)/(\alpha_2 - \alpha_1)$. Then for all integers $n \geqslant 0$, we have $x(n) = c(\alpha_2^{n+1} - \alpha_1^{n+1})$. By Theorem 3, we need only check the case that $|\alpha_1|_p = |\alpha_2|_p$, and we are in the case (3) with $\gamma = \alpha_2/\alpha_1$ and $u = -\gamma$. If there exist an integer l $(0 \leqslant l < p^2\ell)$ and $\theta \in \mathbb{Z}_p$ such that $\varphi_l(\theta) = 1 - \gamma^{l+1} \exp(\ell\theta \log(1 + p\pi\gamma_1 + (\pi\gamma_0)^{p^2})) = 0$, where $\gamma = u_0(1 + \pi\gamma_0)$, then by the unicity of the decomposition, we obtain $u_0^{l+1} = 1$, and thus

$$\exp\bigl(\ell\theta \log\bigl(1 + p\pi\gamma_1 + (\pi\gamma_0)^{p^2}\bigr)\bigr) = \gamma^{-(l+1)} = (1 + \pi\gamma_0)^{-(l+1)}.$$

But $(1 + \pi\gamma_0)^{p^2} = 1 + p\pi\gamma_1 + (\pi\gamma_0)^{p^2}$, thus we have

$$\exp\bigl(\ell p^2\theta \log\bigl(1 + p\pi\gamma_1 + (\pi\gamma_0)^{p^2}\bigr)\bigr) = \exp\bigl(-(l+1)\log\bigl(1 + p\pi\gamma_1 + (\pi\gamma_0)^{p^2}\bigr)\bigr).$$

Therefore $\ell p^2\theta = -(l+1)$, and then $v_p(x)$ is p-regular by Theorem 3. □

Remark. The famous Fibonacci sequence $(F_n)_{n \geqslant 0}$ satisfies $F_1 = F_0 = 1$, and $F_{n+2} = F_{n+1} + F_n$ for all integers $n \geqslant 0$. Thus for any prime number p, the sequence $(v_p(F_n))_{n \geqslant 0}$ is p-regular. This result has been established recently by L.A. Medina and E.S. Rowland [6] via a total different method.

Next we shall consider Lucas sequences which include as famous examples the Fibonacci numbers, Fermat numbers, Mersenne numbers, Pell numbers, Lucas numbers, and Jacobsthal numbers. See for example http://en.wikipedia.org/wiki/Lucas_sequence.

Given $P, Q \in \mathbb{Z} \setminus \{0\}$, the Lucas sequences of the first kind $U_n(P, Q)$ and of the second kind $V_n(P, Q)$ are integer sequences defined by the following recurrence relations, where $n \geqslant 2$ is an integer:

$$U_0(P,Q) = 0, \qquad U_1(P,Q) = 1, \qquad U_n(P,Q) = PU_{n-1}(P,Q) - QU_{n-2}(P,Q),$$
$$V_0(P,Q) = 2, \qquad V_1(P,Q) = P, \qquad V_n(P,Q) = PV_{n-1}(P,Q) - QV_{n-2}(P,Q).$$

Corollary 1. *If $U_n(P, Q) \neq 0$ for all integers $n \geqslant 1$, then $(v_p(U_n(P, Q)))_{n \geqslant 1}$ is p-regular.*

Proof. The result comes directly from Theorem 4 for $U_2(P, Q) = PU_1(P, Q)$. □

Corollary 2. *If $V_n(P, Q) \neq 0$ for all integers $n \geqslant 1$, then $(v_p(V_n(P, Q)))_{n \geqslant 1}$ is p-regular.*

Proof. We shall follow the classification in Theorem 3 and put $x(n) = V_{n+1}(P, Q)$ for all integers $n \geqslant 0$.

Case I: $\alpha_1 = \alpha_2$. Then $\alpha_1 = P/2$, and $a = 0$. Thus $v_p(x)$ is p-regular by Theorem 3.

Case II: $\alpha_1 \neq \alpha_2$. Then $a = \alpha_1$, $b = \alpha_2$, and thus $u = \gamma = \alpha_2/\alpha_1$. As above we need only consider the case (3), and we have $|\alpha_1|_p = |\alpha_2|_p$. If there exist some integer l $(0 \leqslant l < p^2\ell)$ and $\theta \in \mathbb{Z}_p$ such that

$$\varphi_l(\theta) = 1 + \gamma^{l+1} \exp\bigl(\ell\theta \log\bigl(1 + p\pi\gamma_1 + (\pi\gamma_0)^{p^2}\bigr)\bigr) = 0,$$

where $\gamma = u_0(1 + \pi\gamma_0)$, then by the unicity of the decomposition, we obtain $u_0^{2(l+1)} = 1$, and thus

$$\exp\bigl(2\ell\theta \log\bigl(1 + p\pi\gamma_1 + (\pi\gamma_0)^{p^2}\bigr)\bigr) = \gamma^{-(2l+1)} = (1 + \pi\gamma_0)^{-2(l+1)}.$$

But $(1 + \pi\gamma_0)^{p^2} = 1 + p\pi\gamma_1 + (\pi\gamma_0)^{p^2}$, thus we have

$$\exp\bigl(2\ell p^2\theta \log\bigl(1 + p\pi\gamma_1 + (\pi\gamma_0)^{p^2}\bigr)\bigr) = \exp\bigl(-2(l+1) \log\bigl(1 + p\pi\gamma_1 + (\pi\gamma_0)^{p^2}\bigr)\bigr).$$

So $2\ell p^2\theta = -2(l+1)$, and $v_p(x)$ is p-regular by Theorem 3. □

Acknowledgements

Jia-Yan Yao would like to thank the National Natural Science Foundation of China (Grants No. 10671104 and No. 10990011) and the Chern Institute of Mathematics (Tianjin) for partial financial support. Finally we would like to thank heartily the anonymous referee for his pertinent comments and valuable suggestions.

References

[1] J.-P. Allouche, J.O. Shallit, The ring of k-regular sequence, Theoret. Comput. Sci. 98 (1992) 163–197.
[2] J.-P. Allouche, J.O. Shallit, The ring of k-regular sequence II, Theoret. Comput. Sci. 307 (2003) 3–29.
[3] J.-P. Allouche, J.O. Shallit, Automatic Sequences: Theory, Applications, Generalizations, Cambridge University Press, 2003.
[4] Y. Amice, Les Nombres p-adiques, Presses Universitaires de France, 1975.
[5] J.P. Bell, p-adic valuations and k-regular sequences, Discrete Math. 307 (2007) 3070–3075.
[6] L.A. Medina, E.S. Rowland, p-regularity of the p-adic valuation of the Fibonacci sequence, http://arxiv.org/abs/0910.2907.
[7] E. Weiss, Algebraic Number Theory, Dover, 1998.