Available online at http://scik.org
J. Math. Comput. Sci. 11 (2021), No. 2, 1704-1713
https://doi.org/10.28919/jmcs/5384
ISSN: 1927-5307

PERIODICITY OF p-ADIC EXPANSION OF RATIONAL NUMBER

RAFIK BELHADEF[1,*], HENRI-ALEX ESBELIN[2]

[1]LPAM, Department of Mathematics, Mohamed Seddik BenYahia University of Jijel, Algeria
[2]LIMOS, Clermont Auvergne University, Aubière, France

Abstract. In this paper we give an algorithm to calculate the coefficients of the p-adic expansion of a rational numbers, and we give a method to decide whether this expansion is periodic or ultimately periodic.

Keywords: p-adic expansion; p-adic number; rational number.

2010 AMS Subject Classification: 11A07, 11D88, 11Y99.

1. INTRODUCTION

It is known that in $\mathbb{R}$, an element is rational if and only if its decimal expansion is ultimately periodic. An important analogous theorem for the p-adic expansion of rational number, is given by the following statement (see [1]):

Theorem 1.1. *The number $x \in \mathbb{Q}_p$ is rational if and only if the sequence of digits of its p-adic expansion is periodic or ultimately periodic.*

For example, in $\mathbb{Q}_3$, the 3-adic expansion of $-\frac{1}{2}$ is $1+3+3^2+3^3+... = 111111111111$, it is clear that this expansion is purely periodic. In the second example in $\mathbb{Q}_3$, the 3-adic expansion of $\frac{11}{5}$ is given by $1+1.3+1.3^2+2.3^3+1.3^4+0.3^5+... = 1112101210121012101210.....$ This

*Corresponding author
E-mail address: belhadef_rafik@univ-jijel.dz
Received January 03, 2021

expansion is ultimately periodic, with periodic block 1210. Another example in $\mathbb{Q}_5$, the 5-adic expansion of $\frac{213}{7}$ is given by $4+1.5+3.5^2+1.5^3+4.5^4+2.5^5+3.5^6+0.5^7+2.5^8+... =$ 413142302142302... This expansion is ultimately periodic, with periodic block 142302.

Evertse in [3], gave an algorithm to calculate the coefficients of p-adic expansion of an element in $\mathbb{Z}_p$. We continue the study of the characterization of p-adic numbers (see [2]), we inspired by the works of Evertse, we propose the algorithm (1), to calculate the sequence of digits of a rational number $\frac{c}{d}$, then we prove that this sequence defines the p-adic expansion of $\frac{c}{d}$ (see lemma 2.2), and it satisfies the relationship (2) (see lemma 2.3). Finally, in the main theorem, we demonstrate the periodicity of the p-adic expansion of $\frac{c}{d}$.

2. Definitions and Properties

We will recall some definitions and basic facts from p-adic numbers (see [4]). Throughout this paper p is a prime number, $\mathbb{Q}$ is the field of rational numbers, $\mathbb{Q}^+$ is the field of nonnegative rational numbers and $\mathbb{R}$ is the field of real numbers. We use $|.|$ to denote the ordinary absolute value, v_p the p-adic valuation and $|.|_p$ the p-adic absolute value. The field of p-adic numbers $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to the p-adic absolute value. We denote the ring of p-adic integers by $\mathbb{Z}_p$. Every element of $\mathbb{Q}_p$ can be expressed uniquely by the p-adic expansion $\sum_{n=-j}^{+\infty} \alpha_n p^n$ with $\alpha_i \in \{0,1,..,p-1\}$ for $i \geq -j$. In $\mathbb{Z}_p$ we have simply $j=0$.

Now, we give in the following definition the requested algorithm for a rational number

Definition 2.1. Let $\frac{c}{d} \in \mathbb{Q}^+ \cap \mathbb{Z}_p$, with $c \in \mathbb{N}$, $d \in \mathbb{N}^*$, and $(c,p)=1$, $(d,p)=1$, $(c,d)=1$. We define the sequences $(\alpha_i)_{i\in\mathbb{N}}$ and $(\beta_i)_{i\in\mathbb{N}}$ by

$$(1) \qquad \begin{cases} \beta_0 = c \\ \alpha_i = \beta_i d^{-1} \mathrm{mod} p, \forall i \geq 0 \\ \beta_{i+1} = \dfrac{\beta_i - \alpha_i d}{p} \in \mathbb{Z}, \forall i \geq 0 \end{cases}$$

Lemma 2.2. *Under the hypothesis of the definition (2.1), the p-adic expansion of* $\frac{c}{d}$ *is given by* $\sum_{i=0}^{+\infty} \alpha_i p^i$*, with* $\alpha_i \in \{0,1,..,p-1\}$, $\forall i \geq 0$. *The opposite is true, i.e, if* $\frac{c}{d} = \sum_{i=0}^{+\infty} \alpha_i p^i$*, then the sequences* $(\alpha_i)_{i\in\mathbb{N}}$ *and* $(\beta_i)_{i\in\mathbb{N}}$ *satisfies the algorithm (1).*

Proof. Let $(\alpha_i)_{i\in\mathbb{N}}$ and $(\beta_i)_{i\in\mathbb{N}}$ as in the definition (2.1). We have

$$\begin{aligned}
\frac{c}{d} &= \alpha_0 + \frac{\beta_1}{d} p \\
&= \alpha_0 + \alpha_1 p + \frac{\beta_2}{d} p^2 \\
&\dots \\
&= \alpha_0 + \alpha_1 p + \dots + \alpha_n p^n + \frac{\beta_{n+1}}{d} p^{n+1}
\end{aligned}$$

So

$$\left| \frac{c}{d} - \sum_{i=0}^{n} \alpha_i p^i \right|_p \leq \frac{1}{p^{n+1}}$$

therefore $\sum_{i=0}^{+\infty} \alpha_i p^i = \frac{c}{d}$.

For the second part, we suppose $\frac{c}{d} = \sum_{i=0}^{+\infty} \alpha_i p^i$, and we prove by recursion that the sequences $(\alpha_i)_{i\in\mathbb{N}}$ and $(\beta_i)_{i\in\mathbb{N}}$ satisfies the algorithm (1). For $i=0$, we have $\frac{c}{d} = \alpha_0 \text{mod} p$, then $\alpha_0 = cd^{-1}\text{mod} p$. Now, we suppose that $\alpha_i = \beta_i d^{-1}\text{mod} p$ and $\beta_{i+1} = \frac{\beta_i - \alpha_i d}{p}$, so we have

$$\begin{aligned}
\alpha_i = \beta_i d^{-1}\text{mod} p &\Longrightarrow \alpha_{i+1} p + \alpha_i = \beta_i d^{-1}\text{mod} p \\
&\Longrightarrow \alpha_{i+1} p = \left(\beta_i d^{-1} - \alpha_i\right) \text{mod} p \\
&\Longrightarrow \alpha_{i+1} = \left(\frac{\beta_i - \alpha_i}{p}\right) d^{-1}\text{mod} p = \beta_{i+1} d^{-1}\text{mod} p
\end{aligned}$$

therefore $\forall i \geq 0 : \alpha_i = \beta_i d^{-1}\text{mod} p$. □

Lemma 2.3. *Under the hypothesis of the definition (2.1), we have*

$$c = d\left(\sum_{n=0}^{i-1} \alpha_n p^n\right) + \beta_i p^i \quad , \quad \forall i \in \mathbb{N}^* \tag{2}$$

Proof. We prove this lemma, also, by induction. For $i = 1$, it's obvious.

$$d\left(\sum_{n=0}^{0} \alpha_n p^n\right) + \beta_1 p = d\alpha_0 + \left(\frac{c - \alpha_0 d}{p}\right) p = c$$

Suppose that, the relationship is true for i. From (1), we have $\beta_i = \alpha_i d + \beta_{i+1} p$. Then

$$\begin{aligned} c &= d\left(\sum_{n=0}^{i-1} \alpha_n p^n\right) + \beta_i p^i \\ &= d\left(\sum_{n=0}^{i-1} \alpha_n p^n\right) + (\beta_{i+1} p + \alpha_i d)\, p^i \\ &= d\left(\sum_{n=0}^{i} \alpha_n p^n\right) + \beta_{i+1} p^{i+1} \end{aligned}$$

So, the relationship is true for all $i \in \mathbb{N}$. □

Remark 2.4. Let $r = \dfrac{c'}{d'} \in \mathbb{Q}^+$, but not in $\mathbb{Z}_p$, i.e. the p-adic expansion of $\dfrac{c'}{d'}$ is given by $\sum\limits_{n=-j}^{+\infty} \alpha_{n+j} p^n$, with $j \neq 0$ and $\alpha_i \in \{0, 1, .., p-1\}$, $\forall i \geq -j$. In this case, we can suppose $c' = c \in \mathbb{N}$, $d' = p^j d \in \mathbb{N}^*$, with $(d, p) = 1$, and $(c, p) = 1$. So, we have $\dfrac{c}{d} = \sum\limits_{n=0}^{+\infty} \alpha_n p^n$. We define a sequence $(\beta_i)_{i \in \mathbb{N}}$ by the same way

$$\begin{cases} \beta_0 = c = c' \\ \\ \beta_{i+1} = \dfrac{\beta_i - \alpha_i d}{p} = \dfrac{\beta_i p^j - \alpha_i d'}{p^{j+1}} \in \mathbb{Z} \end{cases} \tag{3}$$

3. Main Results

To show that the algorithm (2.1) stops after a certain rank, it suffices to prove that the sequence $(|\beta_n|)_{n \in \mathbb{N}}$ is bounded or decreasing. This is the subject of the main theorem.

Main Theorem 3.1. *The sequence $(\beta_i)_{i \in \mathbb{N}}$ given in (1) verified the following cases:*

Case1. *If $c < d$, then*

$$0 \leq |\beta_i| < d \quad , \ \forall i \in \mathbb{N}$$

Case2. *If $c > d$ and $p \geq 3$, we have, also, two cases:*

Case2.1. *If $0 < \frac{c(p-1)}{2dp} < 1$, then for all $i \in \mathbb{N}^*$, we have $|\beta_i| < d$.*

Case2.2. *If $1 < \frac{c(p-1)}{2dp}$, then for a fixed integer*

$$m = \left[\frac{\log\left(\dfrac{c(p-1)}{2dp}\right)}{\log p} \right] \tag{4}$$

it comes that

$$\begin{cases} d < |\beta_i| < c & for \quad 0 \le i < m+1 \\ \\ 0 \le |\beta_i| < d & for \qquad m+1 < i \\ \\ 0 \le |\beta_i| < c & for \qquad m+1 = i \end{cases}$$

Proof. We treat all cases:

Case1. Let $c < d$, we use the proof by induction. For $i = 0$ is trivial. We suppose that in the rank n we have $|\beta_i| < d$, and we prove the inequality $|\beta_{i+1}| < d$. Indeed, we have

$$\begin{aligned} |\beta_{i+1}| &= \left|\frac{\beta_i - \alpha_i d}{p}\right| \\ &< \frac{1}{p}|\beta_i| + \frac{1}{p}|\alpha_i d| \\ &< \frac{1}{p}d + \frac{p-1}{p}d = d \end{aligned}$$

Case2. For $c > d$ and $p \ge 3$, we prove the two following cases:

Case2.1. We suppose $0 < \frac{c(p-1)}{2dp} < 1$. Also, we prove by recurrence that $|\beta_i| < d$. Starting with $i = 1$, we have

$$0 < \frac{c(p-1)}{2dp} < 1 \Longleftrightarrow -\frac{\alpha_0 d}{p} < \frac{c}{p} - \frac{\alpha_0 d}{p} < \frac{2d}{p-1} - \frac{\alpha_0 d}{p}$$

So

$$-d < -\frac{\alpha_0 d}{p} < \beta_1 < d\left(\frac{2}{p-1} - \frac{\alpha_0}{p}\right) < d$$

Now, we assume that the property is true at rank i, and we show it at rank $i+1$. Indeed, we have

$$-d < \beta_i < d \Longleftrightarrow -d < \frac{-d\,(1+\alpha_i)}{p} < \frac{\beta_i - \alpha_i d}{p} < \frac{d\,(1-\alpha_i)}{p} < d$$

then $-d < \beta_{i+1} < d$. Which means that for every $i \in \mathbb{N}^*$, we have $|\beta_i| < d$.

Case2.2. Let the integer m given in (4), we suppose that $1 < \dfrac{c(p-1)}{2dp}$.

Firstly, we will prove that for all $0 \le i \le m$ the terms β_i are strictly positive. Indeed, we assume that there is $k \in \{1,...,m\}$, such that $\beta_k < 0$. From definition (2.1), we have

$$\frac{\beta_{k-1} - \alpha_{k-1} d}{p} < 0$$

which means $\beta_{k-1} < dp$. Multiplying both sides by p^{k-1}, and applying the lemma (2.3), it comes

$$c < d\left(\sum_{n=0}^{k-2} \alpha_n p^n\right) + dp^k$$

The coefficients α_n are strictly less than p, so

$$c < dp\left(\frac{p^{k-1}-1}{p-1} + p^{k-1}\right)$$

Then, after simplification

$$c < \frac{pd}{p-1}\left(p^k - 1\right) < \frac{2pd}{p-1}p^k$$

Thus

$$\frac{\log\left(\frac{c(p-1)}{2dp}\right)}{\log p} < k$$

however $m+1 \leq k$. Where does the contradiction come from. Which means that for every $0 \leq i \leq m$, we have $\beta_k > 0$.

Now, we prove the inequalities $d \leq \beta_i \leq c$ for $i \in \{0, ..., m\}$.

The inequality in law is easily proved by recurrence for all $0 \leq i \leq m$. To prove the inequality in the left, we use the absurd. We assume that, there is a positive integer $k \in \{1, ..., m\}$ such that $0 < \beta_k < d$ (the condition $d < c$ implies that $k \neq 0$). By lemma (2.3) we obtain

$$\beta_k < d \iff c < d\left(\sum_{n=0}^{k-1} \alpha_n p^n\right) + dp^k$$

So $c < dp(1 + p + ... + p^{k-1} + p^{k-1})$. Hence

$$c < \frac{dp}{p-1}\left(2p^k - p^{k-1} - 1\right) \iff c < \frac{2pd}{p-1}p^k$$

It comes that

$$\frac{\log\left(\frac{c(p-1)}{2dp}\right)}{\log p} < k$$

However $m+1 \leq k$, hence the contradiction. Which means that for all $0 \leq i \leq m$, we have $c \geq \beta_k \geq d$.

For the second part of this case, we suppose there is a positive integer $k > m+1$ such that $|\beta_k| > d$, that is $\beta_k > d$ or $\beta_k < -d$. By lemma (2.3), we have

$$\beta_k > d \Longleftrightarrow c > d\left(\sum_{n=0}^{k-1} \alpha_n p^n\right) + dp^k > dp^k$$

hence $\frac{c(p-1)}{2dp} > \left(\frac{p-1}{2}\right) p^{k-1} > p^{k-1}$, therefore

$$\frac{\log\left(\frac{c(p-1)}{2dp}\right)}{\log p} > k-1$$

then

$$m+1 = \left\lfloor \frac{\log\left(\frac{c(p-1)}{2dp}\right)}{\log p} \right\rfloor + 1 > k$$

Contradiction. For the second inequality, we have by the formula (1)

$$\beta_k = \frac{\beta_{k-1} - \alpha_k d}{p} \leq -d$$

then $\beta_{k-1} \leq d(\alpha_k - p)$, however $\alpha_k \leq p-1$, thus $\beta_{k-1} \leq -d$. And so on, until $\beta_0 = c \leq -d$, which is another contradiction. So, for all $i \geq m+2$ we have $|\beta_i| \leq d$. The last part is easly.

□

Example 3.2. For $p = 3$, $c = 7$ and $d = 11$, the case 1 is verified (see table 1)

Table 1: Case 1

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
α_k	2	2	0	0	1	1	2	0	0	1	1	2	0	0	1	1
β_k	7	−5	−9	−3	−1	−4	−5	−9	−3	−1	−4	−5	−9	−3	−1	−4

For $p = 3$, $c = 8$ and $d = 5$, the case 2.1 is verified (see table 2)

Table 2: Case 2.1

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
α_k	1	2	0	1	2	1	0	1	2	1	0	1	2	1	0	1
β_k	8	1	−3	−1	−2	−4	−3	−1	−2	−4	−3	−1	−2	−4	−3	−1

For $p = 3$, $c = 17$ and $d = 5$, we have $m = 0$ and the case 2.2 is verified (see table 3)

Table 3: Case 2.2 for m=0

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
α_k	1	2	2	1	0	1	2	1	0	1	2	1	0	1	2	1
β_k	17	4	−2	−4	−3	−1	−2	−4	−3	−1	−2	−4	−3	−1	−2	−4

For $p = 3$, $c = 124$ and $d = 7$, we have $m = 1$ and the case 2.2 is verified (see table 4)

Table 4: Case 2.2 for m=1

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
α_k	1	0	1	2	2	0	1	0	2	1	2	0	1	0	2	1
β_k	124	39	2	−4	−6	−2	−3	−1	−5	−4	−6	−2	−3	−1	−5	−4

For $p = 3$, $c = 247$ and $d = 7$, we have $m = 2$ and the case 2.2 is verified (see table 5)

Table 5: Case 2.2 for m=2

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
α_k	1	2	1	2	0	2	1	2	0	1	0	2	1	2	0	1
β_k	247	80	22	5	−3	−1	−5	−4	−6	−2	−3	−1	−5	−4	−6	−2

In the following corollary, we give a particlar case $p=2$.

Corollary 3.3. *For $p=2$, The sequence $(\beta_i)_{i\in\mathbb{N}}$ given in (1) verified the same cases:*

Cas1. *If $c<d$, then*

$$0 \leq |\beta_i| < d \quad , \quad \forall i \in \mathbb{N}$$

Cas2. : *If $c>d$, we have also two cases:*

Cas2.1. *If $0<\frac{c}{2d}<1$, then for all $i\in\mathbb{N}^*$ we have $|\beta_i|<d$.*

Cas2.2. *If $1<\frac{c}{2d}$, then for a fixed integer*

$$m = \left[\frac{\log\left(\frac{c}{2d}\right)}{\log 2} \right]$$

it comes that

$$\begin{cases} d \leq |\beta_i| \leq c & \textit{for} \quad 0 \leq i < m+1 \\ \\ 0 \leq |\beta_i| \leq d & \textit{for} \qquad m+1 \leq i \\ \\ 0 \leq |\beta_i| < c & \textit{for} \qquad m+1 = i \end{cases}$$

Proof. The proof is similar to that of the main theorem. □

Example 3.4. For $p=2$, $c=5$ and $d=9$, the case 1 is verified (see table 6)

Table 6: Case 1

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
α_k	1	0	1	1	1	0	0	0	1	1	1	0	0	0	1	1
β_k	5	−2	−1	−5	−7	−8	−4	−2	−1	−5	−7	−8	−4	−2	−1	−5

For $p=2$, $c=5$ and $d=3$, the case 2.1 is verified (see table 7)

Table 7: Case 2.1

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
α_k	1	1	1	0	1	0	1	0	1	0	1	0	1	0	1	0
β_k	5	1	−1	−2	−1	−2	−1	−2	−1	−2	−1	−2	−1	−2	−1	−2

For $p = 2$, $c = 7$ and $d = 3$, we have $m = 0$ and the case 2.2 is verified (see table 8)

Table 8: Case 2.2 for m=0

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
α_k	1	0	1	1	0	1	0	1	0	1	0	1	0	1	0	1
β_k	7	2	1	−1	−2	−1	−2	−1	−2	−1	−2	−1	−2	−1	−2	−1

For $p = 2$, $c = 13$ and $d = 3$, we have $m = 1$ and the case 2.2 is verified (see table 9)

Table 9: Case 2.2 for m=1

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
α_k	1	1	1	1	0	1	0	1	0	1	0	1	0	1	0	1
β_k	13	5	1	−1	−2	−1	−2	−1	−2	−1	−2	−1	−2	−1	−2	−1

For $p = 2$, $c = 25$ and $d = 3$, we have $m = 2$ and the case 2.2 is verified (see table 10)

Table 10: Case 2.2 for m=2

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
α_k	1	1	0	0	1	1	0	1	0	1	0	1	0	1	0	1
β_k	25	11	4	2	1	−1	−2	−1	−2	−1	−2	−1	−2	−1	−2	−1

CONFLICT OF INTERESTS

The author(s) declare that there is no conflict of interests.

REFERENCES

[1] G. Bachman, Introduction to p-adic Numbers and Valuation Theory, Academic press, New York and London. 1964.

[2] R. Belhadef, H-A. Esbelin and T. Zerzaihi, Transcendence of Thue-Morse p-adic Continued Fraction, Mediterr. J. Math. 13(2016),1429-1434.

[3] J. H. Evertse, p-adic Numbers, Course Notes, 2011. `http://www.math.leidenuniv.nl/~evertse/dio2011-padic.pdf`.

[4] F. Q. Gouvêa, p-adic numbers: an introduction, 2nd ed, Springer, Berlin; New York, 2003.