A Division Algorithm Approach to p-Adic Sylvester Expansions

Eric Errthum

Department of Mathematics and Statistics
Winona State University
Winona, MN
E-mail: eerrthum@winona.edu

Abstract

A method of constructing finite p-adic Sylvester expansions for all rationals is presented. This method parallels the classical Fibonacci-Sylvester (greedy) algorithm by iterating a p-adic division algorithm. The method extends to irrational p-adics that have an embedding in the reals.

Keywords: p-adic number, p-adic division algorithm, Sylvester series expansion
2010 MSC: 11A67, 11J61

1. Introduction

In [2] and [3] A. Knopfmacher and J. Knopfmacher give algorithms for constructing Egyptian fraction expansions in a p-adic setting that are analogous to those given for the reals by Oppenheim [8]. However, for some positive rational inputs the Knopfmachers' algorithm fails to return a finite expansion. In Section 2 we review the basics of the Knopfmachers' Sylvester-type algorithm and give such an example. We then introduce a modification of their algorithm that will give finite Sylvester expansions for all rationals. The seemingly unnatural correction term in our algorithm is explained by the alternate approach detailed in the final two sections.

In Section 3 we briefly recall the Fibonacci-Sylvester Greedy Algorithm, especially its relationship to the classical division algorithm. This provides the main motivation for Section 4 wherein we define a new p-adic division algorithm and use the same relationship to construct finite rational p-adic Sylvester expansions. Lastly we show that the division algorithm approach

and the given modification to Knopfmachers' algorithm yield the same output.

2. p-Adic Expansions

2.1. Basics of p-Adic Numbers

We begin with some of the necessary basics of p-adic numbers. A more thorough exposition can be found in [4]. Let p be a prime and $\mathbb{Q}_p$ the completion of the rationals with respect to the p-adic absolute value $|\cdot|_p$ defined on $\mathbb{Q}$ by

$$|0|_p = 0 \text{ and } |r|_p = p^{-\nu} \text{ if } r = \frac{a}{b}p^{\nu}, \text{ where } p \nmid ab.$$

The exponent $\nu \in \mathbb{Z}$ is the p-adic valuation, or order, of r and will be denoted $\nu_p(r)$.

Proposition 2.1 (c.f. [4])**.** *Let nonzero $\zeta, \xi \in \mathbb{Q}_p$.*

1. *There exists a unique $\widehat{\zeta} \in \mathbb{Q}_p$ such that $\nu_p\left(\widehat{\zeta}\right) = 0$ and $\zeta = \widehat{\zeta}p^{\nu_p(\zeta)}$. We will call $\widehat{\zeta}$ the unit part of ζ.*
2. $\nu_p(\zeta\xi) = \nu_p(\zeta) + \nu_p(\xi)$.
3. $\nu_p(\zeta + \xi) \geq min\{\nu_p(\zeta), \nu_p(\xi)\}$. *We have equality when $\nu_p(\zeta) \neq \nu_p(\xi)$.*

Every element of $\mathbb{Q}_p$ has the shape

$$\zeta = \sum_{n=\nu_p(\zeta)}^{\infty} c_n p^n \tag{1}$$

for $c_n \in \{0, 1, \ldots, p-1\}$. This representation is unique, however p-adic numbers can also be represented in the form

$$\zeta = a_0 + \sum_{n=1} \frac{1}{a_n} \tag{2}$$

where $a_n \in \mathbb{Z}[\frac{1}{p}]$ and the sum is either finite or converges p-adically. There are a variety of algorithms to decompose a p-adic into this form (c.f. [2]). One reason to study such representations is that they can be considered the p-adic analogue to representing real numbers as Egyptian fractions, i.e. as the sum of unit fractions.

2.2. Sylvester-type Series Expansions of p-Adic Numbers

There are various methods of decomposing a rational number into an Egyptian fraction representation. One of the more naïve methods was given originally by Fibonacci and again in modern times by Sylvester [9]. This algorithm is commonly known as the Greedy Algorithm because at each inductive step of the decomposition one simply takes the largest unit fraction smaller than the value being decomposed. Later, Oppenheim [8] generalized this and other Egyptian fraction algorithms to real numbers given by their decimal representations.

The following inductive algorithm, which results in an expansion like (2), is presented by the Knopfmachers in [2] as a p-adic analogue to the Sylvester-Oppenheim algorithm on real numbers. Begin by defining the fractional part of a p-adic number ζ as in (1) by

$$\langle \zeta \rangle = \sum_{n=\nu_p(\zeta)}^{0} c_n p^n. \tag{3}$$

Algorithm 2.2 ([2])**.** *Let $\zeta \in \mathbb{Q}_p$. For the initial term, set $a_0 = \langle \zeta \rangle$. Then take $\zeta_1 = \zeta - a_0$ so that $\nu_p(\zeta_1) \geq 1$. Continuing as long as $\zeta_n \neq 0$, let*

$$a_n = \left\langle \frac{1}{\zeta_n} \right\rangle \text{ and } \zeta_{n+1} = \zeta_n - \frac{1}{a_n}.$$

In [3] (see Proposition 5.3) it is stated that the above Sylvester-type algorithm and a similarly defined Engel-type algorithm terminate if and only if $\zeta \in \mathbb{Q}$. However in [1] Grabner and A. Knopfmacher give an example of a rational with nonterminating Engel-type algorithm. Likewise, there are rationals for which this Sylvester-type algorithm does not terminate.

Indeed, suppose $\zeta = \frac{a}{p+a} \in \mathbb{Q}$ with $p \nmid a$. Then $a_0 = 1$ and $\zeta_1 < 0$. Since all the a_n are defined to be positive, a finite sum in (2) leads to a contradiction. Although Laohakosol and Kanasri [6] give a complete characterization of the infinite Sylvester-type expansions from the Knopfmachers' algorithm that correspond to rational numbers, it is less obvious the necessary conditions under which a rational will result in a finite expansion.

2.3. A New Sylvester-Type Algorithm

We start by generalizing the definition in (3) in the following way. Let

$$\langle \zeta \rangle_k = \sum_{n=\nu_p(\zeta)}^{k-1} c_n p^n$$

so that $\langle\zeta\rangle_1 = \langle\zeta\rangle$. In other words, $\langle\zeta\rangle_k$ is the rational image of ζ under the mod p^k projection from $\mathbb{Q}_p$ to $\mathbb{Z}[\frac{1}{p}]$.

For real x, define the ceiling function, $\lceil x \rceil$, to be the least integer greater than x. Notice that since $\mathbb{Q}_p$ is not an ordered field, this function is not well-defined for all p-adics. However, if $\zeta \in \mathbb{Q}_p$ such that there exists an embedding of $\mathbb{Q}(\zeta)$ into $\mathbb{R}$, then the ceiling function pulls back to $\mathbb{Q}(\zeta) \subset \mathbb{Q}_p$.

We now state our modification to Algorithm 2.2.

Algorithm 2.3. *Let nonzero $\zeta \in \mathbb{Q}_p$ such that there exists an embedding $\psi : \mathbb{Q}(\zeta) \to \mathbb{R}$ and $k \in \mathbb{Z}$ such that $k > -\nu_p(\zeta)$. Set $\zeta_0 = \zeta$. Inductively for $i \geq 0$ set $t_i = \left\langle \frac{1}{\zeta_i} \right\rangle_k$,*

$$q_i = t_i + \left\lceil \frac{1 - t_i\psi(\zeta_i)}{p^k\psi(\zeta_i)} \right\rceil p^k,$$

and

$$\zeta_{i+1} = \zeta_i - \frac{1}{q_i}. \tag{4}$$

The algorithm terminates if any $\zeta_N = 0$.

Theorem 2.4. *Algorithm 2.3 produces a sequence of $q_i \in \mathbb{Z}[\frac{1}{p}]$ such that*

$$\zeta = \sum_{i=0} \frac{1}{q_i}$$

where the sum (if infinite) converges p-adically.

Proof. By (4), if the sum converges, it does so to ζ. It suffices to show that $|\zeta_i|_p \to 0$.

Suppose $\nu_p(\zeta_i) = s > -k$ so that $\zeta_i = \widehat{\zeta}_i p^s$. Then

$$t_i = \left\langle \frac{1}{\widehat{\zeta}_i} p^{-s} \right\rangle_k = \left\langle \widehat{\zeta}_1^{-1} \right\rangle_{k+s} p^{-s}$$

and

$$q_i = \left(\left\langle \widehat{\zeta}_1^{-1} \right\rangle_{k+s} + mp^{k+s} \right) p^{-s}$$

for some $m \in \mathbb{Z}$. Then

$$\zeta_i q_i - 1 = \widehat{\zeta}_i \left\langle \widehat{\zeta}_1^{-1} \right\rangle_{k+s} + \widehat{\zeta}_i m p^{k+s} - 1 \equiv 0 \mod p^{k+s}$$

so $\nu_p(\zeta_i q_i - 1) \geq k + s$. Then $\nu_p(\zeta_{i+1}) \geq k + s - \nu_p(q_i)$. Since $k > -s$, then $\nu_p(q_i) \geq -s$. Hence, $\nu_p(\zeta_{i+1}) \geq k + 2s > \nu_p(\zeta_i)$. Since the order of the ζ_i is strictly increasing, $|\zeta_i|_p \to 0$. □

Example 2.5. *Let $k = 1$ and consider $\xi \in \mathbb{Q}_7$ with $\xi^2 = \frac{1}{11}$ and $\xi \equiv 4 \mod 7$. Then $\mathbb{Q}(\xi)$ embeds into $\mathbb{R}$ by either $\psi(\xi) = \frac{1}{\sqrt{11}}$ or $\psi(\xi) = \frac{-1}{\sqrt{11}}$. For the first choice, Algorithm 2.3 gives*

$$\xi = \frac{1}{9} + \frac{7}{66} + \frac{7^3}{4709} + \frac{7^7}{72282453} + \cdots.$$

The second embedding yields

$$\xi = \frac{1}{2} + \frac{7}{12} + \frac{7^3}{617} + \frac{7^7}{1045103} + \cdots.$$

Algorithm 2.3 certainly isn't as elegant looking as Knopfmachers' Algorithm and has limitations for which p-adics it can be used on. However the importance of Algorithm 2.3 is in the following theorem.

Theorem 2.6. *Algorithm 2.3 terminates if and only if $\zeta \in \mathbb{Q}$.*

Instead of proving this theorem directly, in the following sections we will re-frame the approach to finding p-adic Sylvester expansions for rationals to mimic a more classical technique. In Section 4.3 we will show the link between the two and the proof of Theorem 2.6 will follow easily.

3. The Fibonacci-Sylvester Greedy Algorithm

The algorithm given by Fibonacci and Sylvester for Egyptian fractions of rationals can be interpretted as iterating a modified version of the classical division algorithm (c.f. [7]). We review these classical methods now to provide reference and motivation for the techniques used later.

Theorem 3.1 (Modifed Classical Division Algorithm)**.** *For all $a, b \in \mathbb{Z}$, $a > 0$, there exist unique q, $r \in \mathbb{Z}$ such that*

$$b = aq - r \tag{5}$$

with

$$0 \leq r < a. \tag{6}$$

Note that Theorem 3.1 is greedy in the sense that it finds the smallest q such that $aq > b$, i.e. so that $\frac{a}{b} > \frac{1}{q}$.

Algorithm 3.2 (F-S Greedy Algorithm)**.** *Let* $-1 < \frac{a}{b} \in \mathbb{Q}$*, with* $a > 0$ *and* $\gcd(a, b) = 1$*. Iterate Theorem 3.1 in the following way:*

$$\begin{aligned} b &= \quad aq_0 - r_0 \\ bq_0 &= \quad r_0 q_1 - r_1 \\ &\vdots \\ bq_0 q_1 \cdots q_{i-1} &= \quad r_{i-1} q_i - r_i \\ &\vdots \end{aligned} \tag{7}$$

The process terminates if any $r_N = 0$*.*

A straightforward computation (c.f. [7]) then gives the following:

Theorem 3.3. *Algorithm 3.2 terminates in a finite number of steps and*

$$\frac{a}{b} = \sum_{i=0}^{N} \frac{1}{q_i}. \tag{8}$$

4. A p-Adic Division Algorithm Approach

4.1. The p^k-Division Algorithm

We begin the process of retracing the classical approach by generalizing Theorem 3.1. The p-adic division algorithm defined here is similar to the one given in [5] but differs considerably in the restrictions on the quotient and remainder.

Theorem 4.1 (p^k-Division Algorithm)**.** *Let* p *be prime and* $k \in \mathbb{Z}$*. For all* $a, b \in \mathbb{Z}[\frac{1}{p}]$*,* $a > 0$*, there exist unique* $q, r \in \mathbb{Z}[\frac{1}{p}]$ *such that*

$$b = aq - r \tag{9}$$

with

$$0 \leq r < ap^k \tag{10}$$

and

$$|r|_p \leq |ap^k|_p. \tag{11}$$

Proof. We first prove existence. Since $\widehat{a}$ and p are relatively prime, positive and negative powers of p are defined mod $\widehat{a}$. Let $\alpha = \nu_p(a)$ and $\beta = \nu_p(b)$ and take $0 \leq \overline{r} < \widehat{a}$ such that $\overline{r} \equiv -\widehat{b}p^{\beta-\alpha-k} \mod \widehat{a}$.
(Case 1: $k > \beta - \alpha$.) For some $m \in \mathbb{Z}$ we have $\overline{r}p^{-\beta+\alpha+k} + \widehat{b} = \widehat{a}m$ which gives

$$\widehat{b}p^{\beta} = \widehat{a}p^{\alpha}mp^{\beta-\alpha} - \overline{r}p^{\alpha+k}.$$

Thus we can take $q = mp^{\beta-\alpha}$ and $r = \overline{r}p^{\alpha+k}$.
(Case 2: $k \leq \beta - \alpha$.) For some $m \in \mathbb{Z}$ we have $\overline{r} + \widehat{b}p^{\beta-\alpha-k} = \widehat{a}m$ which gives

$$\widehat{b}p^{\beta} = \widehat{a}mp^{\alpha+k} - \overline{r}p^{\alpha+k}. \tag{12}$$

Thus we can take $q = mp^k$ and $r = \overline{r}p^{\alpha+k}$.

In both cases, since $\overline{r} < \widehat{a}$, both (10) and (11) are satisfied.

To show uniqueness, suppose that there exist q_1, r_1, q_2, r_2 satisfying (9), (10), and (11). Then

$$a(q_1 - q_2) = r_1 - r_2,$$

thus $r_1 \equiv r_2 \mod \widehat{a}$. Also $r_1 \equiv r_2 \mod p^{\alpha+k}$ since by assumption $\nu_p(r_i) \geq \nu_p\left(ap^k\right)$. Therefore, $r_1 \equiv r_2 \mod ap^k$. Since both are between 0 and ap^k, $r_1 = r_2$. Thus $q_1 = q_2$ and we have uniqueness as desired. □

Note that the value $\overline{r}$ may have nontrivial order. When $\nu_p(\overline{r}) \geq 1$ we say a jump occurs. Of course, if $p > \widehat{a}$ then $\overline{r} = \widehat{r}$ and there is no jump.

Also notice that one recovers Theorem 3.1 from Theorem 4.1 by setting $k = 0$ (or $p = 1$) and (redundantly) using the standard absolute value in (11). Additionally Theorem 4.1 generalizes the classical algorithm in the form of the following corollary.

Corollary 4.2. *Suppose $a, b, p, k \in \mathbb{Z}$ with p prime and $k \leq \nu_p(b) - \nu_p(a)$. Let q_p denote the quotient from the p^k-division algorithm on a and b and let q_∞ denote the quotient from the modified classical division algorithm on ap^k and b. Then $q_p = q_\infty p^k$.*

Proof. Since $k \leq \nu_p(b) - \nu_p(a)$, Case 2 in the proof of Theorem 4.1 applies and $q_p = mp^k$. So it suffices to show that $m = q_\infty$. By (12),

$$0 \leq ap^k m - b < ap^k.$$

Thus (5) and (6) are satisfied. □

In addition, note that the p^k-Division Algorithm can be extended to rational a and b in the following way. Suppose $b = \frac{s}{t}$ and $a = \frac{u}{v}$ for $r, s, t, u \in \mathbb{Z}$. To find the quotient and remainder, clear denominators and compute the desired division algoritm on $b' = sv$ and $a' = ut$ to find q' and r'. Then $q = q'$ and $r = \frac{r'}{vt}$ satisfy (9), (10) and (11). However, since we are mostly interested in the quotient $\frac{a}{b}$, we will assume $a, b \in \mathbb{Z}[\frac{1}{p}]$.

4.2. The p^k-Greedy Algorithm

Since we now have a generalization of Theorem 3.1, we can substitute it into the iterative process of Algorithm 3.2.

Algorithm 4.3 (p^k-Greedy Algorithm)**.** *Let $\frac{a}{b} \in \mathbb{Q}$, with $a > 0$, $\gcd(a, b) = 1$ and $k > -\nu_p\left(\frac{a}{b}\right)$. Iterate Theorem 4.1 as in (7). The process terminates if any $r_N = 0$.*

The condition $k > -\nu_p\left(\frac{a}{b}\right)$ plays the synonymous role to $-1 < \frac{a}{b}$ in the F-S Greedy Algorithm: it prevents the division algorithm from returning a quotient equal to 0. This restriction on k is actually stronger than it needs to be for this alone. However, for reasons related to Corollary 4.2 and explained further below, $k \leq -\nu_p\left(\frac{a}{b}\right)$ is generally undesirable. The Knopfmachers avoided this obstruction by defining their initial a_0 outside of the inductive pattern so that $\nu_p(\zeta_1) \geq 1$. A similar strategy could be used here as well, though we find it more desirable to instead simply choose a different k value.

Theorem 4.4. *Algorithm 4.3 terminates after a finite number of steps.*

Proof. As opposed to Algorithm 3.2, now we have $q_i, r_i \in \mathbb{Z}[\frac{1}{p}]$ instead of $\mathbb{Z}$. However

$$\widehat{r}_i \leq \overline{r}_i < \widehat{r}_{i-1} \in \mathbb{Z},$$

so the sequence of $\widehat{r}_i$'s is a decreasing sequence of positive integers much like the classical remainders. □

Since the algorithm terminates, again we get that (8) holds.

Example 4.5. *Consider $\frac{a}{b} = \frac{473}{25}$. Performing the 3-Greedy Algorithm yields,*

$$\begin{aligned}
25 &= 473 \cdot 2 - 921 \\
25 \cdot 2 &= 921 \cdot \frac{5}{3} - 1485 \\
25 \cdot 2 \cdot \frac{5}{3} &= 1485 \cdot \frac{115}{81} - 2025 \\
25 \cdot 2 \cdot \frac{5}{3} \cdot \frac{115}{81} &= 2025 \cdot \frac{1150}{19683} - 0
\end{aligned}$$

and thus

$$\frac{473}{25} = \frac{1}{2} + \frac{3}{5} + \frac{3^4}{115} + \frac{3^9}{1150}.$$

However, performing the 3^4*-Greedy Algorithm results in the sum*

$$\frac{473}{25} = \frac{1}{23} + \frac{3^4}{5635} + \frac{3^{12}}{28175}.$$

Applying Corollary 4.2 to Algorithm 4.3 gives another relationship between the classical and p-adic algorithms.

Corollary 4.6. *Suppose* $\frac{a}{b} > 0$ *and the situation of* $k \leq -\nu_p\left(\frac{a}{b}\right)$ *holds. If no jumps occur than each term of the* p^k*-Greedy Algorithm for* $\frac{a}{b}$ *is equal to the corresponding term in the F-S Greedy Algorithm on* $\frac{ap^k}{b}$ *divided by* p^k*.*

Example 4.7. *Consider the fraction* $\frac{a}{b} = \frac{5}{121} = \frac{5}{11^2}$*. If we take* $p = 11$ *and* $k = 1$*, then* $k \leq -\nu_{11}\left(\frac{a}{b}\right) = 2$*. Applying the* 11*-Greedy Algorithm to* $\frac{5}{121}$ *encounters no jumps and gives*

$$\frac{5}{121} = \frac{1}{33} + \frac{1}{99} + \frac{1}{1089}.$$

On $\frac{5\cdot 11}{121} = \frac{5}{11}$*, the F-S Greedy Algorithm yields*

$$\frac{5}{11} = \frac{1}{3} + \frac{1}{9} + \frac{1}{99}.$$

The restriction on jumps is sufficient but not necessary. For example, the 3-Greedy Algorithm on $\frac{22}{45}$ encounters a jump, yet the relation above to the classical algorithm on $\frac{22}{15}$ still holds.

Also notice that, again with $k \leq -\nu_p\left(\frac{a}{b}\right)$, if $\frac{ap^k}{b} > 1$ then the F-S Greedy Algorithm returns quotients $q_i = 1$ until the remaining value to be decomposed is less than 1. Hence, by Corollary 4.6 the p^k-Greedy Algorithm on $\frac{a}{b}$ produces a finite string of terms equal to $\frac{1}{p^k}$. For these reasons we only consider the cases where $k > -\nu_p\left(\frac{a}{b}\right)$.

This condition is minor, though, in the grand scheme. Each inductive step of Algorithm 4.3 is independent of each other with respect to the value of k. So if the desired k fails the order criteria, it is possible to temporarily use a sufficiently large k' in the initial step(s) and then switch back to the desired k value once the corresponding orders become large enough. In this way finite p-adic Sylvester expansions can be found for all rationals.

4.3. Connection Between Approaches

We are now in the position to return to the modification of the Knopfmachers' algorithm given in Section 2.

Theorem 4.8. *For $\zeta \in \mathbb{Q}$, Algorithm 2.3 and Algorithm 4.3 produce the same output.*

Proof. Suppose $\zeta_i \in \mathbb{Q}$ for some $i \geq 0$. Then $\zeta_i = \frac{a}{b}$ for a, $b \in \mathbb{Z}$. Algorithm 2.3 produces

$$q_i = \left\langle \frac{b}{a} \right\rangle_k + \left\lceil \frac{b/a - \langle b/a \rangle_k}{p^k} \right\rceil p^k.$$

Let $r = aq_i - b$ and $\sigma_k = \left\langle \frac{b}{a} \right\rangle_k - \frac{b}{a}$. Then

$$0 \leq \frac{r}{a} = \sigma_k + \left\lceil \frac{-\sigma_k}{p^k} \right\rceil p^k < p^k.$$

Since $\nu_p(\sigma_k) \geq k$, then $|r|_p \leq |ap^k|_p$. Hence both (10) and (11) are satisfied. □

The proof of Theorem 2.6 is simply a combination of Theorem 4.4 and Theorem 4.8. Further the condition of $k > -\nu_p(\zeta)$ in Algorithm 2.3 is explained in light of Corollary 4.6. Indeed, for negative or irrational ζ with $k \leq -\nu_p(\zeta)$, a statement analogous to Corollary 4.6 holds and thus Algorithm 2.3 produces a p-adically divergent result. Though, as mentioned above, this can be worked around by temporarily using alternate k-values.

Acknowledgements

Thank you to Anthony Martino for being the first to convince me that Egyptian fractions are interesting and for helping me work out parts of Sections 4.1 and 4.2 in the $k = 1$ case.

This work is dedicated to my children, Gedion and Eomji.

[1] Grabner, Peter J.; Knopfmacher, Arnold. *Arithmetic and metric properties of p-adic Engel series expansions.* Publ. Math. Debrecen 63 (2003), no. 3, 363-377.

[2] Knopfmacher, A.; Knopfmacher, J. *Series expansions in p-adic and other non-Archimedean fields.* J. Number Theory 32 (1989), no. 3, 297-306.

[3] Knopfmacher, A.; Knopfmacher, J. *Infinite series expansions for p-adic numbers*, J. Number Theory 41 (1992), no. 2, 131-145.

[4] Koblitz, N. "p-adic Numbers, p-adic Analysis, and Zeta-Functions." Graduate Texts in Mathematics 58, Springer, New York, 1977.

[5] Lager, C. *A p-adic Euclidean Algorithm*, Rose-Hulman Undergraduate Mathematics Journal 10 (2009), no. 2.

[6] Laohakosol, V.; Kanasri, N. R. *A characterization of rational numbers by p-adic Sylvester series expansions*, Acta Arith. 130 (2007), no. 4, 389-402.

[7] Mays, M. *A worst case of the Fibonacci-Sylvester expansion*, J. Combin. Math. Combin. Comput. 1 (1987), 141-148.

[8] Oppenheim, A. *The representation of real numbers by infinite series of rationals*, Acta Arith. 21 (1972) 391-398.

[9] Sylvester, J. J. *On a Point in the Theory of Vulgar Fractions.* Amer. J. Math. 3 (1880), no. 4, 332-335.