P-adic Continued Fractions

Matthew Moore

December 7, 2005

Abstract

Continued fractions in $\mathbb{R}$ have a single definition and algorithms for approximating them are well known. There also exists a well known result which states that $\sqrt{m}$, $m \in \mathbb{Q}$, always has a periodic continued fraction representation. In $\mathbb{Q}_p$, the field of p-adics, however, there are competing and non-equivalent definitions of continued fractions and no single algorithm exists which always produces a periodic continued fraction for $\sqrt{m}$. In Jerzy Browkin's 1978 and 2000 papers, *Continued Fractions in Local Fields, I* and *II*, respectively, Browkin presents two definitions for a p-adic continued fraction and presents several algorithms for computing continued fraction approximations to p-adic square roots with the end-goal of finding periodic continued fraction expansions. This paper will serve as an introduction to p-adic numbers and as an exploration of the definitions and algorithms associated with p-adic continued fractions.

1 Definitions

Definition: Cauchy Sequence: Let $\{x_n\}_{n\in\mathbb{N}}$ be a sequence. Then, $\{x_n\}_{n\in\mathbb{N}}$ is a *Cauchy Sequence* if

for all $\epsilon > 0$ there exists $N \in \mathbb{N}$ such that, for all $n \geq N$, $|x_n - x_{n+1}| < \epsilon$.

Note that the summation of a *Cauchy Sequence*, $\sum_{i=0}^{\infty} x_i$, converges.

Definition: Valuation: Let K be a field. A valuation on K is a function $|\cdot| : K \longrightarrow \mathbb{R}$ with the following properties:

1. $|a| \geq 0$ for all $a \in K$, and $|x| = 0$ if and only if $x = 0$.
2. $|a * b| = |a| \cdot |b|$ for all $a, b \in K$.

3. $|a+b| \le |a| + |b|$ for all $a, b \in K$.

Specifically, if we take $K = \mathbb{Q}$, then $a \in \mathbb{Q}$ can be written as $a = \frac{a'}{b} p^n$ for a prime p where p does not divide a or b. The valuation $|\cdot|_p$ is then given by:

$$|x|_p := \begin{cases} \frac{1}{p^n} & \text{if } x \neq 0, \\ 0 & \text{if } x = 0. \end{cases}$$

Definition: Metric: A metric space is a space K with a function $d : K \times K \longrightarrow \mathbb{R}$ such that:

1. $d(x, y) \ge 0$, for all $x, y \in K$.
2. $d(x, y) = d(y, x)$, for all $x, y \in K$.
3. $d(x, z) \le d(x, y) + d(y, z)$, for all $x, y, z \in K$.

In particular, it can be shown that $|a-b|_p$ is a valuation on $\mathbb{Q}_p$, for $a, b \in \mathbb{Q}_p$.

Definition: Completion: Let K be a metric space with a metric d. Let $\bar{K}$ be the set of all Cauchy sequences in K. We then define the equivalence relation between Cauchy sequences, $\sim$, as $x_n \sim y_n$ if the sequence $\{x_0, y_0, x_1, y_1, \ldots, x_n, y_n, \ldots\}$ is also a Cauchy sequence. Let $\hat{K}$ be the set of all equivalence classes in $\bar{K}$. The metric d then extends like so:

$$d(\{x_n\}, \{y_n\}) = \lim_{n \to \infty} d(x_n, y_n).$$

$\hat{K}$ is called the *completion* of K.

Definition: $\mathbb{Q}_p$: Given a prime p, the p-adic integers, $\mathbb{Z}_p$, are obtained by taking the completion of $\mathbb{Z}$ with respect to the metric induced by the valuation $|\cdot|_p$. The field of *p-adic rationals*, $\mathbb{Q}_p$, is the fraction field of $\mathbb{Z}_p$. Note that, as a result of the definition of completion, all $\alpha \in \mathbb{Q}_p$ can be written

$$\alpha = \sum_{i=-r}^{\infty} a_i \cdot p^i, \ a_i \in \{1, 2, \ldots, p-1\}. \tag{1}$$

Definition: Real Continued Fraction: A *real continued fraction* is a fraction of the form

$$a_0 + \cfrac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \ldots}}},$$

with $a_i \in \mathbb{R}$.

Definition: p-adic Continued Fraction: Browkin presents two non-equivalent definitions of a *p-adic continued fraction.* The first resembles the definition of a real continued fraction:

$$\alpha = b_0 + \frac{a_0}{b_1 + \frac{a_1}{b_2 + \frac{a_2}{b_3 + \dots}}},$$

with $b_i \in \{1, 2, \dots, p-1\}$, $a_i = p^{\alpha \cdot j}$, and $a_i \geq 1$ for $i \geq 1$. The second definition instead assumes that $a_i = 1$ for $i \geq 0$ and

$$b_i \in \mathbb{Z}\left[\frac{1}{p}\right] \cap \left(-\frac{p}{2}, \frac{p}{2}\right) = \{-\frac{p-1}{2}, \dots, -1, 0, 1, \dots, \frac{p-1}{2}\}$$

2 Algorithms for Continued Fractions

For $\alpha \in \mathbb{Q}_p$, with α given as in (1), define the map $s : \mathbb{Q}_p \longrightarrow \mathbb{Q}$ to be

$$s(\alpha) = \sum_{i=-r}^{0} a_i \cdot p^i, \ a_n \in \{0, \pm 1, \dots, \pm\frac{p-1}{2}\}. \tag{2}$$

The first algorithm presented procedes as in the classical definition of a real continued fraction.

2.1 Algorithm I

Given $\alpha \in \mathbb{Q}_p$, we define inductively sequences $\{a_n\}$ and $\{b_n\}$ as follows:

[Step 1] $i = 0$. `Let` $a_0 = \alpha$ `and` $b_0 = s(\alpha)$.

[Step 2] `If` $a_i = b_i$ `then` a_{i+1} `and` b_{i+1} `are undefined. If this is the case, quit the algorithm.`

[Step 3] $i = i + 1$. `Let` $a_i = (a_{i-1} - b_{i-1})^{-1}$ `and` $b_i = s(a_i)$. `Go to Step 2.`

The resulting sequence $\{b_n\}$, $n \in \mathbb{N}$, is defined to be the p-adic continued fraction of α.

For $\alpha \in \mathbb{Q}_p$, define

$$s_1(\alpha) = s(\alpha) = \sum_{i=-r}^{0} a_i \cdot p^i \text{ and } s_1'(\alpha) = s_1(\alpha) - p \cdot sign(s_1(\alpha)),$$

with a_i as in (2). Similarly, define

$$s_n(\alpha) \sum_{i=-r}^{-1} a_i \cdot p^i \text{ and } s_2'(\alpha) = s_2(\alpha) - sign(s_2(\alpha)).$$

With these two new definitions in hand, we define the next algorithm.

2.2 Algorithm II

Let $s_1'' = s_1$ and

$$s_2''(\alpha) = \begin{cases} s_2(\alpha) & v(\alpha - s_2(\alpha)) = 0 \\ s_2'(\alpha) & \text{otherwise} \end{cases}$$

Where v is the p-adic valuation. Given $\alpha \in \mathbb{Q}_p$, we define inductively sequences $\{a_n\}$ and $\{b_n\}$ as follows:

[Step 1] $i = 0$ `Let` $a_0 = \alpha$ `and` $b_0 = s_1''(a_0)$`.`

[Step 2] `If` $a_i = b_i$`, then` a_i `and` b_i `are undefined. If this is the case, quit the algorithm.`

[Step 3] $i = i + 1$`. Let` $a_i = (a_{i-1} - b_{i-1})^{-1}$ `and` $b_i = s_2''(a_i)$`.`

[Step 4] `If` $a_i = b_i$`, then` a_i `and` b_i `are undefined. If this is the case, quit the algorithm.`

[Step 5] $i = i + 1$`. Let` $a_i = (a_{i-1} - b_{i-1})^{-1}$ `and` $b_i = s_1''(a_i)$`. Go to Step 2.`

Continuing in this manner, using s_1'' for even i and s_2'' for odd i, we obtain a sequence $\{b_n\}$, $n \in \mathbb{N}$. This sequence is the p-adic continued fraction of α.

3 Additional Algorithms

3.1 Evaluating a Continued Fraction

When finding continued fraction representations of numbers, it is useful to have a way to evaluate these continued fractions. Thus, a standard algorithm for evaluating continued fractions is introduced:

$$\text{Define: } \frac{A_n}{B_n} = [b_0, b_1, \ldots, b_n].$$

With

$$\begin{array}{lll} A_0 = b_0, & A_1 = b_0 \cdot b_1 + 1, & A_n = b_n \cdot A_{n-1} + A_{n-2}, \text{ for } n \geq 2, \\ B_0 = 1, & B_1 = b_1, & B_n = b_n \cdot B_{n-1} + B_{n-2}, \text{ for } n \geq 2. \end{array}$$

Then the fraction $\frac{A_n}{B_n}$ is the evaluated continued fraction approximation of a number. The true usefulness of this algorithm becomes apparent when it is necessary to evaluate a continued fracton as it is computed. A situation in which this is necessary will soon arise.

3.2 Period Detection

In order to test for the periodicity of continued fraction expansions, a search algorithm is required. Thus, a standard linear period search algorithm was implemented:

> Starting with a window size of 1, the window is positioned over a part of the sequence and what is contained in the window is scanned into memory. What has been scanned is then compared to other parts of the sequence to detect if it is repeated. If this fails for the initial position, the position is offset by 1, and the process repeats. If this fails for all positions, the window size is increased by 1 and the position is reset to the initial starting point. If this fails for all combinations of window position and window size, the sequence is decided to not have a period.

3.3 Periodicity Prediction

The problem with using the standard continued fraction algorithm (Algorithm I) in $\mathbb{Q}_p$ is that the floor function is not clearly defined. Algorithm II as well as III and IV (not appearing in this paper) are still the standard algorithm, but with slightly more sophisticated floor functions. The implementation of these floor functions is made more complex by Browkin's choice of p-adic integers:

$$\mathbb{Z}_p = \mathbb{Z}\left[\frac{1}{p}\right] \cap \left(-\frac{p}{2}, \frac{p}{2}\right) = \{-\frac{p-1}{2}, \ldots, -1, 0, 1, \ldots, \frac{p-1}{2}\}.$$

Since this choice of $\mathbb{Z}_p$ is not natively supported by any computational number systems, various work-arounds had to be developed. While attemping to implement the floor function and to debug it, I noticed that when using a particular floor function, the continued fractions produced were either very close to the desired number, or very far away. I also noticed that the cases when the continued fraction evaluated to a very close number was when the continued fractions had a period. This led to the redesign of Algorithm I with the focus on only the evaluation and not the sequence representing the continued fraction.

The floor function which produced this was the following:

For $\alpha \in \mathbb{Q}_p$; $\alpha = \sum_{i=-r}^{\infty} a_i \cdot p^i$, with $a_i \in \mathbb{Z}_p = \{0, 1, \dots, p-1\}$.
If $\sum_{i=-r}^{0} a_i \cdot p^i > \frac{p-p^r}{2}$, then return $-p + \sum_{i=-r}^{0} a_i \cdot p^i > \frac{p-p^r}{2}$ as the floor of α.

The partial sum is compared to $\frac{p-p^r}{2} = \sum_{i=-r}^{0} \frac{p-1}{2} \cdot p^i$ since any number greater than the summation will have a negative representation for $i = 0$ in Browkin's definition.

4 Data

4.1 Periodic Continued Fractions

In Browkin's 2000 paper, he presented data for continued fractions of $\sqrt(m)$, for $1 \leq m \leq 100$. The data that I have gathered agrees with his for the displayed results; however, I went further and analyzed the continued fractions for periods for $\sqrt(m)$, $m \leq 10000$. The following is the list of periodic continued fractions found during this search($m \leq 100$ are omitted):

4.1.1 Algorithm I

```
sqrt(104): Period begins at term 3 and is 6 terms long:
List([9/5, -11/5, 12/5, -11/5, 9/5, -49/25])

sqrt(111): Period begins at term 3 and is 10 terms long:
List([-2/5, 2/5, -9/5, 1/5, 4/5, 2/5, -2/5, 9/5, -1/5, -4/5])

sqrt(119): Period begins at term 3 and is 14 terms long:
List([6/5, 9/5, 2/5, -6/5, -7/5, -8/5, 12/5, -6/5, -9/5, -2/5,
      6/5, 7/5, 8/5, -12/5])

sqrt(819): Period begins at term 3 and is 24 terms long:
List([-3/5, -3/5, -7/5, -7/5, -7/5, -3/5, -3/5, -2/5, -2/5,
      -4/5, -44/25, 6/5, -129/125, -1/5, -8/5, 4632/3125,
      -8/5, -1/5, -129/125, 6/5, -44/25, -4/5, -2/5, -2/5])

sqrt(1014): Period begins at term 3 and is 8 terms long:
```

```
List([-8/5, 3/5, -2/5, -11/5, 7/5, -4/5, -9/5, -8/5])

sqrt(1139): Period begins at term 3 and is 6 terms long:
List([-12/5, 4/25, -42/25, 54/125, -9/5, -8/5])

sqrt(1439): Period begins at term 3 and is 34 terms long:
List([-9/5, -2/5, 2/5, -2/5, 9/5, -6/5, 12/5, 1/5, -3/5, 1/5,
      12/5, -6/5, 9/5, -2/5, 2/5, -2/5, -9/5, 7/5, 6/5, -6/5,
      1/5, -38/25, -6/5, -9/5, -7/5, 133/125, -7/5, -9/5, -6/5,
      -38/25, 1/5, -6/5, 6/5, 7/5])

sqrt(1596): Period begins at term 3 and is 14 terms long:
List([3/5, 8/5, -2/5, 31/25, -9/5, 22/125, 12/5, -3/5, -8/5,
      2/5, -31/25, 9/5, -22/125, -12/5])

sqrt(2079): Period begins at term 3 and is 8 terms long:
List([53/25, -4/5, -7/5, -7/25, -4/5, 3/5, -11/5, -62/25])

sqrt(3864): Period begins at term 3 and is 8 terms long:
List([-8/5, -279/125, -8/5, -3/5, -4/5, 3471/3125, -4/5, -3/5])

sqrt(7719): Period begins at term 3 and is 12 terms long:
List([8/5, 1/5, 11/5, 1/5, 8/5, -7/5, 3/5, -8/5, 61/125, -8/5,
      3/5, -7/5])
```

4.1.2 Algortihm II

```
sqrt(104): Period begins at term 2 and is 12 terms long:
List([1/25, -1, 1/5, -1, -1/5, -1, -2/5, -1, -1/5, -1, 1/5,
      -1])

sqrt(109): Period begins at term 7 and is 96 terms long:
List([1, 2/5, -2, -2/5, 2, 1/5, 2, 1/5, -1, -1/5, -1, 4/5, -1,
      -1/5, -1, 1/5, 2, 1/5, 2, -2/5, -2, 2/5, 1, 2/5, 1, -1/5,
      -1, -1/5, -1, 11/25, 1, -2/5, 1, 4/5, -1, -2/5, 1, -2/5,
      -1, 23/25, -1, 4/5, -1, -3/5, 1, 1/5, 1, -2/5, 1, -21/25,
      1, -8/25, 1, 2/5, 1, -2/5, -1, 1/5, -1, -6/25, 2,
      116/125, -1, -2/5, 1, -2/5, 1, -2/5, 1, 2/5, 1, -1/5, 2,
      -1/5, -1, 1/5, -1, 1/5, -2, -2/5, -1, -2/25, -1, -2/5, 1,
      -4/5, 1, -3/25, -1, 2/5, -1, -1/5, -1, -1/5, -2, -3/5])

sqrt(114): Period begins at term 3 and is 10 terms long:
List([1, 2/5, -1, 2/5, 1, -1/5, 1, 1/5, -1, -4/5])

sqrt(116): Period begins at term 2 and is 18 terms long:
```

```
List([-1/5, 2, 1/5, 2, -2/5, -1, -2/5, 1, -2/5, 1, -2/5, -1,
      -2/5, 2, 1/5, 2, -1/5, 2])

sqrt(126): Period begins at term 2 and is 2 terms long:
List([2/125, 2])

sqrt(129): Period begins at term 19 and is 6 terms long:
List([-1, 4/5, -1, -1/5, -2, 3/5])

sqrt(136): Period begins at term 41 and is 18 terms long:
List([-1, -1/5, -2, -12/25, -1, 2/5, 2, -1/5, -2, 11/25, -2,
      -1/5, 2, 2/5, -1, -12/25, -2, -1/5])

sqrt(139): Period begins at term 2 and is 6 terms long:
List([2/5, -1, -8/25, 2, -1/5, -1])

sqrt(149): Period begins at term 31 and is 54 terms long:
List([1, 2/5, 2, 1/5, -1, -1/5, 1, -4/5, 1, 56/125, 2, 1/5, 2,
      1/5, 2, 1/5, -1, 1/5, -1, 2/5, -1, -9/25, -2, -2/5, 2,
      -4/5, 1, -1/5, 2, 2/5, -2, 2/5, 2, -3/5, 1, -1/5, -2,
      -4/5, 1, -1/5, -2, 1/5, -1, 1/5, 1, 1/5, -1, -2/5, 1,
      -8/25, 1, -2/5, 2, -3/5])
```

The list of periodic continued fractions observed goes on for Algorithm II, however it is too extensive to be reproduced here. The m such that $\sqrt{m}$ has a periodic continued fraction in Algorithm II are as follows:

```
6, 11, 14, 21, 24, 26, 29, 31, 34, 51, 54, 56, 61, 69, 79,
84, 91, 104, 109, 111, 114, 116, 126, 129, 136, 139, 149,
156, 161, 171, 176, 206, 221, 224, 244, 249, 251, 254, 269,
296, 311, 319, 336, 349, 371, 374, 381, 389, 394, 411, 446,
454, 456, 474, 496, 499, 511, 524, 536, 549, 556, 561, 579,
624, 626, 659, 696, 704, 711, 714, 741, 819, 831, 836, 851,
854, 861, 869, 909, 944, 979, 986, 1001, 1056, 1094, 1096,
1111, 1136, 1141, 1199, 1219, 1224, 1226, 1239, 1251, 1291,
1304, 1331, 1341, 1371, 1401, 1404, 1439, 1476, 1494, 1499,
1551, 1566, 1569, 1599, 1609, 1644, 1651, 1671, 1689, 1721,
1729, 1771, 1786, 1821, 1824, 1866, 1896, 1904, 1914, 1916,
1949, 1966, 1976, 1991, 2046, 2056, 2076, 2099, 2126, 2131,
2139, 2196, 2219, 2224, 2231, 2246, 2259, 2261, 2279, 2281,
2286, 2314, 2326, 2399, 2409, 2426, 2436, 2439, 2441, 2466,
2474, 2496, 2531, 2536, 2604, 2614, 2629, 2636, 2639, 2699,
2716, 2724, 2726, 2731, 2744, 2754, 2764, 2781, 2814, 2819,
2869, 2894, 2926, 2954, 2981, 3021, 3036, 3039, 3104, 3114,
3116, 3126, 3146, 3154, 3166, 3174, 3251, 3284, 3299, 3341,
3346, 3411, 3419, 3426, 3441, 3456, 3474, 3506, 3659, 3784,
```

```
3791, 3796, 3814, 3816, 3856, 3861, 3941, 3951, 3999, 4039,
4106, 4121, 4161, 4289, 4291, 4314, 4326, 4331, 4334, 4379,
4389, 4431, 4484, 4506, 4519, 4606, 4704, 4709, 4726, 4771,
4776, 4824, 4881, 4909, 4944, 4984, 5024, 5119, 5159, 5204,
5229, 5249, 5254, 5276, 5301, 5304, 5311, 5344, 5424, 5456,
5466, 5481, 5506, 5551, 5666, 5701, 5714, 5781, 5814, 5856,
5936, 5951, 5961, 5976, 5979, 6054, 6059, 6174, 6186, 6191,
6221, 6246, 6251, 6276, 6279, 6304, 6309, 6329, 6361, 6369,
6454, 6459, 6474, 6496, 6559, 6636, 6706, 6801, 6819, 6826,
6841, 6959, 6961, 6976, 7034, 7106, 7126, 7259, 7284, 7319,
7349, 7359, 7386, 7419, 7476, 7489, 7494, 7496, 7521, 7556,
7564, 7576, 7581, 7656, 7741, 7746, 7786, 7866, 7871, 7876,
7879, 7896, 7906, 7909, 7956, 8034, 8059, 8071, 8074, 8086,
8129, 8141, 8161, 8199, 8201, 8246, 8294, 8301, 8334, 8354,
8441, 8466, 8541, 8546, 8596, 8606, 8639, 8749, 8754, 8804,
8829, 8921, 8924, 8996, 9026, 9069, 9231, 9246, 9344, 9411,
9446, 9479, 9691, 9714, 9746, 9751, 9819, 9864, 9874, 9906,
9914, 9929
```

4.2 Results of Predictive Algorithm

The following are the numbers whose continued fraction expansion converges for the specialized floor function outlined above:

```
6, 11, 14, 21, 24, 34, 54, 69, 74, 76, 94, 99, 104, 111,
119, 819, 1014, 1139, 1439, 1596, 2079, 2711, 3864, 4054,
7719.
```

Note that these are exactly those numbers (less than 10000) for which Algorithm I produces periodic continued fraction expansions. Furthermore, the analysis performed for Algorithm I above required approximately 6 days of computation. The analysis performed using this predictive algorithm required approximately 45 minutes.

5 Thanks

I would like to thank Dr. Duncan A. Buell for making my research possible through a very generous scholarship.
To Dr. Duncan A. Buell: Through the course of this semester I have been researching p-adic continued fractions. Before the start of this project, I had no concept of a p-adic number and no experience with the type of computing necessary for this project. Now, at the end of this semester of research, I have an understanding of p-adic numbers and greater experience

in computational mathematics. Furthermore, I have had the opportunity to experience mathematical research and gain an insight into what I will be doing in the future. All of these experiences have greatly enriched my semester and given me a much greater understanding of what to expect in graduate school. Furthermore, the financial contribution which was made possible by you has allowed me to devote more time and energy to my other mathematics classes: group theory and real analysis.

I would like to sincerely, thank you for providing the financial backing to allow this entire process to take place. It has been greatly appreciated, and I hope that you have enjoyed reading my paper.

Sincerely, Matthew Moore

6 References

I would like to thank Ben Levitt for many useful conversations and for directing my research.

1. Browkin, Jerzy. "Continued Fractions in Local Fields, I". *Demonstratio Math.* Vol. 11 (1978): 67-82.

2. Browkin, Jerzy. "Continued Fractions in Local Fields, II". *Mathematics of Computation.* Vol. 70, No. 235: 1281-1292.

3. Gouvêa, Fernando Q. *P-adic Numbers: an Introduction.* Springer, 2003.

4. Koblitz, Neal. *P-adic Numbers, P-adic Analysis, and Zeta-Functions.* New York : Springer-Verlag: Graduate Texts in Mathematics: 1977.