

p-adic Arithmetic

Stany De Smedt

The *p*-adic numbers were introduced by K. Hensel in 1908 in his book *Theorie der algebraischen Zahlen*, Leipzig, 1908. In this article we present a package that does *p*-adic calculations using *Mathematica*. It allows addition, subtraction, multiplication, and division of *p*-adic numbers written in Hensel expansion. Functions, such as sqrt, log, exp, sin, cos, sinh, and cosh, are defined using their power series expansion. We also calculate the coefficients of a continuous function with respect to the Mahler and Vanderput bases, and implement the *p*-adic Newton method.

■ Introduction

Let *p* be a prime number, fixed once and for all. If *x* is any rational number other than 0, we can write *x* in the form $x = p^n \frac{a}{b}$, where *a*, *b* ∈ ℤ are relatively prime to *p* and *n* ∈ ℤ. We now define $|x|_p = p^{-n}$ and $|0|_p = 0$, and $\text{ord}_p(x) = n$ and $\text{ord}_p(0) = +\infty$. They satisfy the following properties.

1. $|x|_p \geq 0$, $|x|_p = 0$ if and only if $x = 0$.
2. $|x + y|_p \leq \max\{|x|_p, |y|_p\}$ (the strong triangle inequality) with $|x + y|_p = \max\{|x|_p, |y|_p\}$ if $|x|_p \neq |y|_p$ (the isosceles triangle principle).
3. $|x \cdot y|_p = |x|_p \cdot |y|_p$.

With ord_p instead of $|\cdot|_p$, we get for 2 and 3:

$$\begin{aligned}\text{ord}_p(x + y) &\geq \min\{\text{ord}_p(x), \text{ord}_p(y)\} \\ \text{ord}_p(x \cdot y) &= \text{ord}_p(x) + \text{ord}_p(y)\end{aligned}$$

$|\cdot|_p$ is called the *p*-adic valuation; $\text{ord}_p(\cdot)$ is called the *p*-adic order.

Ostrowski proved that each nontrivial valuation on the field of rational numbers is equivalent either to the absolute value function or to some *p*-adic valuation.

Recall that two valuations $|\cdot|_1$ and $|\cdot|_2$ are equivalent if there exists a positive constant *c* such that $|\cdot|_2 = |\cdot|_1^c$. For a proof of this theorem, see [1].

The completion of the field ℚ of rational numbers with respect to the *p*-adic valuation $|\cdot|_p$ is called the field of *p*-adic numbers and will be denoted \mathbb{Q}_p . The set $\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid |x|_p \leq 1\}$ is the ring of *p*-adic integers.

It can be easily proved that each p -adic number x can be written in the form

$$x = \sum_{n=-f}^{\infty} a_n p^n,$$

where each a_n is one of the elements $0, 1, \dots, p-1$, and $f \in \mathbb{Z}$. This is called the *Hensel representation* of the p -adic numbers. Sometimes one uses, analogous to the ordinary decimal notation for real numbers, the notation

$$a_{-f} \dots a_{-3} a_{-2} a_{-1} a_0, a_1 a_2 \dots a_{n-1} a_n \dots$$

It is this representation, preceded with $\langle p \rangle$ to denote the p -adic, that we will use in our package.

With this representation, one obtains for $x \in \mathbb{Q}_p$:

$$\text{ord}_p(x) = \begin{cases} +\infty & \text{if } a_i = 0 \text{ for all } i, \\ \min \{s \mid a_s \neq 0\} & \text{otherwise,} \end{cases}$$

and

$$|x|_p = p^{-\text{ord}_p(x)}.$$

The set of values of $|\cdot|_p$ is $\{0\} \cup \{p^n \mid n \in \mathbb{Z}\}$, and $\{p^n \mid n \in \mathbb{Z}\} = \{|x|_p \mid x \in \mathbb{Q}_p \setminus \{0\}\}$ is called the *valuation group* of \mathbb{Q}_p .

Every $x \in \mathbb{Z}_p$ can be written as $x = \sum_{n=0}^{\infty} a_n p^n$ with $a_n \in \{0, 1, \dots, p-1\}$. The elements with $a_n = 0$ for sufficiently large n can be identified with the nonnegative integers. Thus $\mathbb{N} \subset \mathbb{Z}_p$ and \mathbb{Z}_p also contains \mathbb{Z} as a subset. For example,

$$-1 = (p-1) + (p-1)p + (p-1)p^2 + \dots$$

Note also that every nonzero element x of \mathbb{Q}_p can be written as $p^n y$, where $n \in \mathbb{Z}$ and $y \in \mathbb{Z}_p$ with $|y|_p = 1$. And just as with decimal fractions, a p -adic number $x = \sum_{i=N}^{\infty} a_i p^i$ is rational if and only if the sequence of the digits a_i is periodic from some index i on.

Due to the strong triangle inequality, we may use the following property, which is much easier than in the Archimedean case:

$$\sum_{i=1}^{\infty} a_i \text{ converges if and only if } \lim_{i \rightarrow \infty} a_i = 0.$$

In general we say that a sequence a_1, \dots, a_n, \dots in \mathbb{Q}_p converges to a if and only if $\lim_{n \rightarrow \infty} |a_n - a|_p = 0$ and we will write this as $\lim_{n \rightarrow \infty} a_n = a$.

For \mathbb{Z}_p and \mathbb{Q}_p we have the following topological properties, which we only present here for completeness.

1. \mathbb{Z}_p is compact: each covering by means of open sets has a finite subcovering.

2. \mathbb{Z}_p is complete: every Cauchy sequence converges.
3. \mathbb{Z} is dense in \mathbb{Z}_p : each element of \mathbb{Z}_p is the limit of elements of \mathbb{Z} .
4. \mathbb{Q}_p is locally compact: each point has a compact neighborhood.
5. \mathbb{Q} is dense in \mathbb{Q}_p .
6. \mathbb{Q}_p is complete and separable: it has a countable dense subset.
7. \mathbb{Q}_p is zero-dimensional: every neighborhood of a point contains an open and closed subset.
8. \mathbb{Q}_p is totally disconnected: the only subsets that are connected as a metric space are the empty set and the singletons.

We now survey the different parts that are treated in this package. For more information on p -adic calculus, see [1] or [2].

■ p-adic Order and Valuation

This is the implementation of the previously defined functions ord_p and $|\cdot|_p$. `PadicOrder[s,p]` returns the number of times that p divides s , roughly speaking.

$$\text{PadicValue}[s, p] = 1 / p^{\text{PadicOrder}[s, p]}$$

Here are some examples.

```
In[1]:= Get["PadicArithmetic.m"];
```

```
In[2]:= PadicOrder[3/16,2]
```

```
Out[2]= -4
```

```
In[3]:= PadicValue[144, 3]
```

```
Out[3]= 1/9
```

■ Conversion to p-adics

Next we calculate the Hensel expansion of a p -adic number to a given precision. One may think of `PadicN[n,p,k]` as being a bit like `N[n,k]`. The internal representation is given as `PadicRational[m,n,e,p]`. `PadicN[n,p]` gives an eight-digit p -adic number; `PadicN[n,p,k]` gives k digits. The numbers to the right of the radix point represent the positive (> 0) powers, and the numbers to the left represent the negative (≤ 0) powers.

The implementation to print these expansions is made in the third section of the package entitled "Printing of p -adics" where we use `PadicDigits[m,n,e,p]` as an auxiliary function to aid formatting.

Here are some examples.

```
In[4]:= PadicN[102356, 3, 12]
Out[4]= <3> 2 . 2 2 1 0 1 2 1 0 2 1 0

In[5]:= PadicN[1/6, 2, 10]
Out[5]= <2> 1 1 . 0 1 0 1 0 1 0 1

In[6]:= PadicN[17/1024, 2]
Out[6]= (<2>1 . 0 0 0 1 0 0 0)  $\frac{1}{2^{10}}$ 

In[7]:= PadicN[125048, 20, 6]
Out[7]= <20> 8 . 12 12 15 0 0
```

■ Basic p -adic Arithmetic

Addition and multiplication of p -adic numbers are defined in several cases whether or not both numbers are given in Hensel expansion. Note that addition and multiplication in \mathbb{Q}_p can be defined by

$$\sum_{n=N}^{\infty} a_n p^n + \sum_{n=M}^{\infty} b_n p^n = \sum_{n=\min\{N,M\}}^{\infty} (a_n + b_n) p^n,$$

$$\left(\sum_{n=N}^{\infty} a_n p^n \right) \left(\sum_{n=M}^{\infty} b_n p^n \right) = \sum_{n=N+M}^{\infty} \left(\sum_{i=N}^{n-M} a_i b_{n-i} \right) p^n.$$

The left-hand expansions are Hensel expansions, but the right-hand ones, in general, are not.

Also p -adic exponentiation is implemented for the case of integer powers. We then define the p -adic version of some classical functions, such as log, exp, sin, cos, sinh, and cosh. This is done with the help of their power series expansions, which are completely analogous to the real case except that their regions of convergence might differ [1]. We have also defined square roots. The existence of square roots of a number x in \mathbb{Q}_p depends on the following theorems.

Let $p \neq 2$. A p -adic number $x = \sum_{i=0}^{\infty} a_i p^i$ ($0 \leq a_i \leq p-1$, $a_0 \neq 0$) is a square if and only if a_0 is a square residue mod p .

Let $p = 2$. A 2-adic number x , $|x|_2 = 1$ is a square if and only if $x \equiv 1 \pmod{8}$.

Finally, we implement the p -adic Gamma function.

Here are some examples.

```
In[8]:= PadicN[10, 3, 5]
Out[8]= <3> 1 . 0 1 0 0
```

```
In[9]:= PadicN[20, 3, 8]
Out[9]= <3> 2 . 0 2 0 0 0 0 0
In[10]:= % + %
Out[10]= <3> 0 . 1 0 1 0 0
In[11]:= PadicN[15, 5] + 17
Out[11]= <5> 2 . 1 1 0 0 0 0 0 0
In[12]:= PadicN[15, 5] * 17
Out[12]= <5> 0 . 1 0 2 0 0 0 0 0
In[13]:= PadicN[9, 2, 10] 2
Out[13]= <2> 0 . 1 0 0 1 0 0 0 0 0 0
In[14]:= PadicN[4, 3, 4]
Out[14]= <3> 1 . 1 0 0
In[15]:= Exp[%]
```

Exp::overflow : Number not in the region of convergence

```
In[16]:= Log[%%]
Out[16]= <3> 0 . 1 2 1 2 2
In[17]:= PadicN[15, 3, 4]
Out[17]= <3> 0 . 2 1 0 0
In[18]:= Exp[%]
Out[18]= <3> 1 . 2 1 0 1
In[19]:= PadicN[-1, 3, 4]
Out[19]= <3> 2 . 2 2 2
In[20]:= Sqrt[%]
```

Sqrt::nonexistence : Square root does not exist

```
In[21]:= PadicN[31, 5, 10]
Out[21]= <5> 1 . 1 1 0 0 0 0 0 0 0
In[22]:= Sqrt[%]
Out[22]= <5> 1 . 3 3 2 2 0 4 1 4 2 1
In[23]:= PadicGamma[15, 3]
Out[23]= -44844800
```

```
In[24]:= PadicGamma[-2, 3]
Out[24]=  $\frac{1}{2}$ 
```

■ Booleans and Selectors on p -adic Rationals

Here we implement whether or not a given number is a p -adic number. The second example selects the different parts of a p -adic number. Next we implement the conversion of a p -adic number to a rational number. We also define the function `SqrtQ[x, p]` to test whether the square roots of x exist in \mathbb{Q}_p or not.

Here are some examples.

```
In[25]:= PadicN[12, 3, 5] / PadicN[4, 3, 3]
Out[25]= <3> 0 . 1 0 0

In[26]:= PadicToRational[%]
Out[26]= 3

In[27]:= PadicExponent[%]
Out[27]= 1

In[28]:= SqrtQ[-1, 3]
Out[28]= False
```

■ Function Expansion

For the space $C(\mathbb{Z}_p \rightarrow \mathbb{Q}_p)$ of all continuous functions from \mathbb{Z}_p to \mathbb{Q}_p (we can simply transfer the definitions from classical analysis to non-Archimedean analysis by adapting the valuations), there exist two well-known bases. On the one hand, we have the *Mabler basis*, consisting of the polynomials $\binom{x}{n}$, $n \in \mathbb{N}$. On the other hand, there is the *Vanderput basis*, consisting of locally constant functions $e_n(x)$, where $e_0(x) = 1$ and for $n \neq 0$, e_n is the characteristic function of the open ball with center n and radius $\frac{1}{n}$. Each continuous function $f: \mathbb{Z}_p \rightarrow \mathbb{Q}_p$ can then be written as

$$f(x) = \sum_{n=0}^{\infty} a_n \binom{x}{n} \quad \text{with} \quad a_n = \sum_{j=0}^n (-1)^{n-j} \binom{n}{j} f(j),$$

$$f(x) = \sum_{n=0}^{\infty} a_n e_n(x) \quad \text{with} \quad a_0 = f(0) \quad \text{and} \quad a_n = f(n) - f(n_-) \quad \text{for} \quad n \neq 0.$$

Here n_- is defined as follows. For every $n \in \mathbb{N}_0$, there exists a p -adic expansion $n = a_0 + a_1 p + \dots + a_N p^N$ with $a_N \neq 0$. Then $n_- = a_0 + a_1 p + \dots + a_{N-1} p^{N-1}$.

In this section of the package we implement these expansions as `Mahler[f,x,n]` and `Vanderput[f,x,n,p]`, which calculate the first $n + 1$ coefficients of the function $f(x)$ according to the respective basis. Note that the Vanderput expansion depends on p , while the Mahler expansion does not.

Here are some examples.

`In[29]:= Mahler[x3 + x + 1, x, 5]`

0 : 1
1 : 2
2 : 6
3 : 6
4 : 0
5 : 0

`In[30]:= Vanderput[x3 + x + 1, x, 5, 3]`

0 : 1
1 : 2
2 : 10
3 : 30
4 : 66
5 : 120

In[31]:= **Vanderput**[$x^3 + x + 1$, x , 5, 5]

0 : 1
1 : 2
2 : 10
3 : 30
4 : 68
5 : 130

■ VolkenbornIntegral

This is the p -adic equivalent of the classical integral. The *Volkenbornintegral* is defined as

$$\int_{\mathbb{Z}_p} f(x) dx = \lim_{n \rightarrow \infty} p^{-n} \sum_{k=0}^{p^n-1} f(k)$$

or equivalently

$$\int_{\mathbb{Z}_p} f(x) dx = \sum_{n=0}^{\infty} \frac{(-1)^n}{n+1} \Delta^n f(0).$$

Here Δ is the *forward difference quotient*: $\Delta f(x) = f(x+1) - f(x)$ and $\Delta^n f(x) = \Delta(\Delta^{n-1} f(x))$. We used this last expression for our implementation.

■ p -adic Newton Method

Here we implement the well-known *Newton method* to solve an algebraic equation $f(x) = 0$. The algorithm is the same as in the classical case, that is, we use the iterations

$$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}.$$

The main problem is to find an appropriate starting value since convergence might be rather slow. We tried to solve this based on the following theorem.

Let $F(x)$ be a polynomial with p -adic integer coefficients and let there exist $\gamma \in \mathbb{Z}_p$, such that $F(\gamma) \equiv 0 \pmod{p}$ and $F'(\gamma) \not\equiv 0 \pmod{p}$. Then there exists $\alpha \in \mathbb{Z}_p$, such that $F(\alpha) = 0$ and $\alpha \equiv \gamma \pmod{p}$.

Here is an example.

In[32]:= `PadicNewton[x^2 - 1, x, 2, 0.0001, 3]`

Out[32]= `<3> 2 . 2 2 2 2 2 2 2 2`

■ References

- [1] W. Schikhof, *Ultrametric Calculus: An Introduction to p-adic Analysis*, New York: Cambridge University Press, 1984.
- [2] N. Koblitz, *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, London: Springer-Verlag, 1977.
- [3] S. Wolfram, *The Mathematica Book*, 5th ed., Champaign: Wolfram Media, Inc., 2003.

■ Additional Material

PadicArithmetic.m

Available at www.mathematica-journal.com.

Stany De Smedt
KBC Bank & Verzekeringen
Havenlaan 12, 1080 Brussels, Belgium