P-ADIC ARITHMETIC

Stany De Smedt

Abstract

This package is meant to do p-adic calculations. It allows addition, subtraction, multiplication and division of p-adic numbers written in Hensel expansion. Also functions as log, exp, sin, cos, sinh and cosh are defined using their power series expansion. At the end, we included a part to calculate the coefficients of a continuous function with regard to the Mahler and Vanderput base.

Introduction

The *p-adic numbers* were introduced by K. Hensel in 1908 in his book "Theorie der algebraïschen Zahlen" (Leipzig, 1908). We denote $\mathbb{Z}_p$ for the ring of *p-adic integers* (i.e. the numbers of the form $\sum_{i=0}^{+\infty} a_i p^i$ with $0 \leq a_i \leq p-1$) and $\mathbb{Q}_p$ for the field of p-adic numbers, i.e. the quotient field of $\mathbb{Z}_p$. Each p-adic number $x \in \mathbb{Q}_p$ can be written as $x = \sum_{i=-\infty}^{+\infty} a_i p^i$ with $0 \leq a_i \leq p-1$. This is called the *Hensel expansion* or *p-adic expansion* of x. The p-adic numbers are sometimes, analogous to the ordinary decimal notation for real numbers, also denoted by

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

It is this representation, preceded with <p> to denote the p-adic, that we will use in our package.

The *p-adic order* of $x = \sum_{i=-\infty}^{+\infty} a_i p^i$ is the smallest m for which $a_m \neq 0$.

More precisely,

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

The *p-adic valuation* of x is defined as $|x|_p = p^{-\mathrm{ord}_p(x)}$ and has the following properties.

i) $|x|_p \geq 0$, $|x|_p = 0$ if and only if $x = 0$

ii) $|x+y|_p \leq \max \{ |x|_p , |y|_p \}$ (the strong triangle inequality)
with $|x+y|_p = \max \{ |x|_p , |y|_p \}$ if $|x|_p \neq |y|_p$
(the isosceles triangle principle)

iii) $|x \,.\, y|_p = |x|_p \,.\, |y|_p$

We now survey the different parts that are treated in this package. For more information on p-adic calculus, we refer to [Schikhof, 1984] or [Koblitz, 1977]

p-adic order and valuation

This is the implementation of the above defined functions ord_p and $|\ |_p$. `PadicOrder[s,p]` returns the number of times that p divides s roughly speaking.
`PadicValue[s,p] = 1/p^(PadicOrder[s,p])`

Examples

```
In[1] : PadicOrder[3/16,2]
Out[1] : -4
In[2] : PadicValue[144,3]
Out[2] : 1/9
```

Conversion to p-adics

In this part 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]`, only evaluating to give a p-adic number in Hensel expansion with a given precision. The internal representation is given as `PadicRational[m,n,e,p]`. `PadicN[n,p]` gives an 8 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, the numbers to the left represent the negative (<= 0) powers.
The implementation to print these expansions is made in a third part called "Printing of p-adics" where we use `PadicDigits[m,n,e,p]` as an auxiliary function to aid formatting.

Examples

```
In[3] : PadicN[102356,3,12]
Out[3] : <3> 2 . 2 2 1 0 1 2 1 0 2 1 0
In[4] : PadicN[1/6,2,10]
Out[4] : <2> 1 1 . 0 1 0 1 0 1 0 1
In[5] : PadicN[17/1024,2]
Out[5] : <2> 1 . 0 0 0 1 0 0 0  2^-10
In[6] : PadicN[125048,20,6]
Out[6] : <20> 8 . 12 12 15 0 0
```

Basic p-adic arithmetic

Addition and multiplication of p-adic numbers is defined is several cases whether or not both numbers are given in Hensel expansion. Also p-adic exponentation is implemented for the case of integer powers.
The next part treats 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 expansion regarding to their region of convergence as it

can be found in [Schikhof, 1984]. Also the implementation of the p-adic Gamma function is made.

Examples

```
In[7] : PadicN[10,3,5]
Out[7] : <3> 1 . 0 1 0 0
In[8] : PadicN[20,3,8]
Out[8] : <3> 2 . 0 2 0 0 0 0 0
In[9] : % + %%
Out[9] : <3> 0 . 1 0 1 0 0
In[10] : PadicN[15,5] + 17
Out[10] : <5> 2 . 1 1 0 0 0 0 0
In[11] : PadicN[15,5] * 17
Out[11] : <5> 0 . 1 0 2 0 0 0 0 0
In[12] : PadicN[9,2,10]^2
Out[12] : <2> 1 . 0 0 0 1 0 1 0 0 0
In[13] : PadicN[4,3,4]
Out[13] : <3> 1 . 1 0 0
In[14] : Exp[%]
Out[14] : Exp::overflow: Number not in the region of convergence
In[15] : Log[%%]
Out[15] : <3> 0 . 1 2 1 2 2
In[16] : PadicN[15,3,4]
Out[16] : <3> 0 . 2 1 0 0
In[17] : Exp[%]
Out[17] : <3> 1 . 2 1 0 1
In[18] : PadicGamma[15,3]
Out[18] : -44844800
In[19] : PadicGamma[-2,3]
Out[19] : 1/2
```

Booleans and Selectors on p-adic rationals

These small parts implement some fancy stuff such as in the first one, the question whether or not a given number is a p-adic number. The second selects the different parts of a p-adic number. Also the conversion of a p-adic number to a rational number is implemented here.

Examples

```
In[20] : PadicN[12,3,5] / PadicN[4,3,3]
Out[20] : <3> 0 . 1 0 0
In[21] : PadicToRational[%]
Out[21] : 3
In[22] : PadicExponent[%%]
Out[22] : 1
```

Function expansion

For the space $C(\mathbb{Z}_p \to \mathbb{Q}_p)$ of all continuous functions from $\mathbb{Z}_p$ to $\mathbb{Q}_p$ there exist two well-known bases. On one hand we have the *Mahler base*,

consisting of the polynomials $\binom{x}{n}$ ($n \in \mathbb{N}$). On the other hand there is the *van der Put base* 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 $f : \mathbb{Z}_p \to \mathbb{Q}_p$ can then be written as

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

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

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

This last section of the package is the implementation of 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 base. Remark that the expansion regarding to the van der Put base depends on p, while the Mahler expansion doesn't.

Examples

```
In[23] : Mahler[x^3+x+1,x,5]
Out[23] : 0 : 1
          1 : 2
          2 : 6
          3 : 6
          4 : 0
          5 : 0
In[24] : Vanderput[x^3+x+1,x,9,3]
Out[24] : 0 : 1
          1 : 2
          2 : 10
          3 : 30
          4 : 66
          5 : 120
          6 : 222
          7 : 348
          8 : 510
          9 : 738
In[25] : Vanderput[x^3+x+1,x,9,5]
Out[25] : 0 : 1
          1 : 2
          2 : 10
          3 : 30
          4 : 68
          5 : 130
          6 : 220
          7 : 340
          8 : 490
          9 : 670
```

References

[Koblitz, 1977] N. Koblitz, P-adic Numbers, P-adic Analysis and Zeta-Functions, Springer-Verlag, 1977

[Schikhof, 1984] W. Schikhof, Ultrametric Calculus : An introduction to p-adic analysis, Cambridge University Press, 1984

Biography

Stany De Smedt was born in 1966 in Merchtem (Belgium) and has been working at the Free University of Brussels since 1988. His main interest lies in p-adic analysis, more specific the study of the continuous and continuously differentiable functions on which he made his doctoral dissertation. He also has a great interest in computer applications of mathematics.

Stany De Smedt
Faculty of Applied Sciences
Vrije Universiteit Brussel
Pleinlaan 2
1050 Brussel
email : sdesmedt@is1.vub.ac.be