Computations with p-adic numbers in Maxima

Jose A Vallejo

Facultad de Ciencias

Universidad Autonoma de San Luis Potosi (Mexico)

http://galia.fc.uaslp.mx/~jvallejo

email:jvallejo@fc.uaslp.mx

Abstract: This is just a first attempt to create a Maxima package for working with p-adic numbers. It is extremely ugly and slow, lacking anything remotely resembling elegance or optimization, but at least it gives correct answers (for all those examples that I have been able to find in the literature).

The current version is suitable for basic courses on the subject of p-adic analysis, and maybe for constructiong examples of some simple theoretical constructions.

Topics covered are:

1. p-adic norm and distance
2. Finite-segment representations of Q_p (Hensel codes)
3. p-adic arithmetic
4. Conversion from Hensel codes to rational functions
5. Newton's method and square roots in Q_p
6. p-adic systems of linear equations

REMARK: Some functions in the package make use of the commands firstn and lastn, which require a Maxima version 5.41 or higher.

1 Loading the package

The most simple way to do it consists in putting a copy of padics.mac in your working directory. If a wxMaxima worksheet is opened from that directory, you can load the package with

(% i1) load("padics.mac");

(% o1)

padics.mac

The other option is to do a global installation, putting a copy of padics.mac in /usr/share/maxima/5.42.1/share/contrib or its Windows equivalent. Then, load the package with the same command above.

2 p-adic norm

We can compute the p-adic order of a rational number with padicorder. The syntax is padicorder(rational,prime):

(% i2) padicorder(144,3);

(% o2) $$2$$

(% i3) padicorder(17,3);

(% o3) $$0$$

We follow the convention that the order of 0 is always (real) infinity:

(% i4) makelist(padicorder(0,i),i,[2,3,5,7,11,13]);

(% o4) $$[\infty, \infty, \infty, \infty, \infty, \infty]$$

(% i5) padicorder(3/10,5);

(% o5) $$-1$$

(% i6) padicorder(36015/88,7);

(% o6) $$4$$

Notice that the p-adic order is an even function:

(% i7) padicorder(-3/10,5);

(% o7) $$-1$$

The reduction to the canonical form of a rational number

r=a/b=p^porder(r) a'/b'

can be achieved with padiccan. The result has the form of a list

[p^porder(r),a'/b']

(% i8) padiccan(0.234,2);

(% o8) $$[\frac{1}{4}, \frac{117}{125}]$$

(% i9) padiccan(0,3);

(% o9) $$[1, 0]$$

The p-adic norm of a rational numer is computed by padicnorm:

(% i10) makelist(padicnorm(0,j),j,[2,3,5,7,11,13,17]);

(% o10) $$[0, 0, 0, 0, 0, 0, 0]$$

(% i11) padicnorm(17,17);

(% o11) $$\frac{1}{17}$$

(% i12) padicnorm(144,3);

(% o12) $$\frac{1}{9}$$

(% i13) padicnorm(12,5);

(% o13) $$1$$

(% i14) makelist(padicnorm(162/13,k),k,[3,13]);

(% o14) $$[\frac{1}{81}, 13]$$

The next example comes from http://mathworld.wolfram.com/p-adicNorm.html

(% i15) makelist(padicnorm(140/297,k),k,[2,3,5,7,11]);

(% o15) $$[\frac{1}{4}, 27, \frac{1}{5}, \frac{1}{7}, 11]$$

Another example, this one from www.asiapacific-mathnews.com/03/0304/0001_0006.pdf

(% i16) makelist(padicnorm(63/550,k),k,[2,3,5,7,11,13]);

(% o16) $$[2, \frac{1}{9}, 25, \frac{1}{7}, 11, 1]$$

(% i17) padicnorm(0.234,2);

(% o17) $$4$$

Let us check the triangle equality:

(% i18) padicnorm(3/10,5);

(% o18) $$5$$

(% i19) padicnorm(40,5);

(% o19) $$\frac{1}{5}$$

(% i20) padicnorm(3/10-40,5);

(% o20) $$5$$

The next examples come from https://www.sangakoo.com/en/unit/p-adic-distance

(% i21) padicnorm(10/12,2);

(% o21) $$2$$

(% i22) padicnorm(10/12,5);

(% o22) $$\frac{1}{5}$$

(% i23) padicnorm(10/12,7);

(% o23) $$1$$

Of course, once we have a norm available, we can define the associated p-adic distance, here denoted padicdist:

(% i24) padicdist(2,28814,7);

(% o24) $$\frac{1}{2401}$$

(% i25) padicdist(2,3,7);

(% o25) $$1$$

(% i26) padicdist(2166^2,2,7);

(% o26) $$\frac{1}{2401}$$

(% i27) padicdist(3,3+29^4,29);

(% o27) $$\frac{1}{707281}$$

The next example comes from https://www.sangakoo.com/en/unit/p-adic-distance

(% i28) padicdist(82,1,3);

(% o28) $$\frac{1}{81}$$

3 p-adic expansions (Hensel codes)

The only explicit representation we can get are those of rational numbers (periodic p-adic expansions). Here we consider Hensel (pseudo)codes, which basically are truncations of the p-adic expansions to a given order. The output has the form [[exponent],mantissa], and the algorithm used here is based on the one proposed by G. Bachman in [1].

(% i29) hensel(5/7,7,7);

(% o29) $$[[-1], 5, 0, 0, 0, 0, 0, 0]$$

(% i30) hensel(-84,7,9);

(% o30) $$[[1], 2, 5, 6, 6, 6, 6, 6, 6, 6]$$

(% i31) hensel(8/3,5,9);

(% o31) $$[[0], 1, 2, 3, 1, 3, 1, 3, 1, 3]$$

(% i32) hensel(3/4,5,4);

(% o32) $$[[0], 2, 1, 1, 1]$$

(% i33) hensel(2/15,5,7);

(% o33) $$[[-1], 4, 1, 3, 1, 3, 1, 3]$$

(% i34) hensel(7/6,5,4);

(% o34) $$[[0], 2, 4, 0, 4]$$

(% i35) hensel(2/7,5,4);

(% o35) $$[[0], 1, 2, 1, 4]$$

(% i36) hensel(1/12,5,7);

(% o36) $$[[0], 3, 4, 2, 4, 2, 4, 2]$$

(% i37) hensel(5/8,5,4);

(% o37) $$[[1], 2, 4, 1, 4]$$

(% i38) hensel(1/2,5,4);

(% o38) $$[[0], 3, 2, 2, 2]$$

(% i39) hensel(1/3,5,4);

(% o39) $$[[0], 2, 3, 1, 3]$$

(% i40) hensel(1/4,5,4);

(% o40) $$[[0], 4, 3, 3, 3]$$

(% i41) hensel(1/4,5,7);

(% o41) $$[[0], 4, 3, 3, 3, 3, 3, 3]$$

(% i42) hensel(1/25,5,4);

(% o42) $$[[-2], 1, 0, 0, 0]$$

(% i43) hensel(-7/8,3,5);

(% o43) $$[[0], 1, 2, 1, 2, 1]$$

The command nicehensel displays the result in the form commonly found in textbooks and expository works (this form has the drawback that, when p>7, is is impossible to distinguish between the number 11 and two consecutive 1's, so it will not be used in what follows), that is, something like

r = a_-e...a_-1.a_0a_1a_2...

where e is the order of r.

(% i44) nicehensel(8/3,5,9);

(% o44)

.123131313

(% i45) nicehensel(8/75,5,9);

(% o45)

12.3131313

(% i46) nicehensel(3/4,5,4);

(% o46)

.2111

(% i47) nicehensel(2/15,5,7);

(% o47)

4.131313

(% i48) nicehensel(1/3,5,7);

(% o48)

.2313131

(% i49) nicehensel(-1/3,5,7);

(% o49)

.3131313

(% i50) nicehensel(5/1,5,4);

(% o50)

.0100

(% i51) nicehensel(25,5,4);

(% o51)

.0010

(% i52) nicehensel(2/7,5,4);

(% o52)

.1214

Let us compare this with the table presented in [2]

(% i53) h[i,j]:=nicehensel(i/j,5,4)$

(% i54) genmatrix(h,17,17);

(% o54)

$$\begin{pmatrix}
.1000 & .3222 & .2313 & .4333 & 1.000 & .1404 & .3302 & .2414 & .4201 & 3.222 & .1332 & .3424 & .2034 & .4101 & 2.313 & .1234 & .3043 \\
.2000 & .1000 & .4131 & .3222 & 2.000 & .2313 & .1214 & .4333 & .3012 & 1.000 & .2120 & .1404 & .4014 & .3302 & 4.131 & .2414 & .1132 \\
.3000 & .4222 & .1000 & .2111 & 3.000 & .3222 & .4021 & .1303 & .2313 & 4.222 & .3403 & .4333 & .1143 & .2013 & 1.000 & .3104 & .4121 \\
.4000 & .2000 & .3313 & .1000 & 4.000 & .4131 & .2423 & .3222 & .1124 & 2.000 & .4240 & .2313 & .3123 & .1214 & 3.313 & .4333 & .2210 \\
.0100 & .0322 & .0231 & .0433 & .1000 & .0140 & .0330 & .0241 & .0420 & .3222 & .0133 & .0342 & .0203 & .0410 & .2313 & .0123 & .0304 \\
.1100 & .3000 & .2000 & .4222 & 1.100 & .1000 & .3142 & .2111 & .4131 & 3.000 & .1411 & .3222 & .2232 & .4021 & 2.000 & .1303 & .3342 \\
.2100 & .1322 & .4313 & .3111 & 2.100 & .2404 & .1000 & .4030 & .3432 & 1.322 & .2204 & .1202 & .4212 & .3222 & 4.313 & .2042 & .1431 \\
.3100 & .4000 & .1231 & .2000 & 3.100 & .3313 & .4302 & .1000 & .2243 & 4.000 & .3041 & .4131 & .1341 & .2423 & 1.231 & .3222 & .4420 \\
.4100 & .2322 & .3000 & .1433 & 4.100 & .4222 & .2214 & .3414 & .1000 & 2.322 & .4324 & .2111 & .3321 & .1134 & 3.000 & .4402 & .2024 \\
.0200 & .0100 & .0413 & .0322 & .2000 & .0231 & .0121 & .0433 & .0301 & .1000 & .0212 & .0140 & .0401 & .0330 & .4131 & .0241 & .0113 \\
.1200 & .3322 & .2231 & .4111 & 1.200 & .1140 & .3423 & .2303 & .4012 & 3.322 & .1000 & .3020 & .2430 & .4431 & 2.231 & .1421 & .3102 \\
.2200 & .1100 & .4000 & .3000 & 2.200 & .2000 & .1330 & .4222 & .3313 & 1.100 & .2332 & .1000 & .4410 & .3142 & 4.000 & .2111 & .1240 \\
.3200 & .4322 & .1413 & .2433 & 3.200 & .3404 & .4142 & .1241 & .2124 & 4.322 & .3120 & .4424 & .1000 & .2343 & 1.413 & .3340 & .4234 \\
.4200 & .2100 & .3231 & .1322 & 4.200 & .4313 & .2000 & .3111 & .1420 & 2.100 & .4403 & .2404 & .3034 & .1000 & 3.231 & .4030 & .2323 \\
.0300 & .0422 & .0100 & .0211 & .3000 & .0322 & .0402 & .0130 & .0231 & .4222 & .0340 & .0433 & .0114 & .0201 & .1000 & .0310 & .0412 \\
.1300 & .3100 & .2413 & .4000 & 1.300 & .1231 & .3214 & .2000 & .4432 & 3.100 & .1133 & .3313 & .2143 & .4302 & 2.413 & .1000 & .3401 \\
.2300 & .1422 & .4231 & .3433 & 2.300 & .2140 & .1121 & .4414 & .3243 & 1.422 & .2411 & .1342 & .4123 & .3013 & 4.231 & .2234 & .1000
\end{pmatrix}$$

4 Arithmetic of p-adics

The basic functions are implemented as:

- padicsum (sum, addition)
- padicsubstract (difference, substraction)
- padicmult (product, multiplication)
- padivdiv (division, quotient) The syntax is quite evident: each function takes the arguments

  (operand1,operand2,p)

Some test numbers:

(% i55) l1:hensel(3/10,5,4);

(l1) $$[[-1], 4, 2, 2, 2]$$

(% i56) l2:hensel(1/2,5,4);

(l2) $$[[0], 3, 2, 2, 2]$$

(% i57) padicsum(l1,l2,5);

(% o57) $$[[-1], 4, 0, 0, 0]$$

Notice that the Hensel code for the sum 3/10+1/1 corresponds to 4/5:

(% i58) hensel(4/5,5,4);

(% o58) $$[[-1], 4, 0, 0, 0]$$

Also, notice that a conequence of using a finite segment representation is that adding up a really small number with a relly big one just gives the bigger:

(% i59) padicsum([[2],2,5,1,5],[[-3],3,3,3,2],7);

(% o59) $$[[-3], 3, 3, 3, 2]$$

Another test (this is an example in [2]) with p=5 and r=9

(% i60) h1:hensel(2/3,5,9);

(h1) $$[[0], 4, 1, 3, 1, 3, 1, 3, 1, 3]$$

(% i61) h2:hensel(5/6,5,9);

(h2) $[[1], 1, 4, 0, 4, 0, 4, 0, 4, 0]$

(% i62) padicsum(h1,h2,5);

(% o62) $[[0], 4, 2, 2, 2, 2, 2, 2, 2, 2]$

Let us check the following example in [2]:

(% i63) padicsubstract(h1,h2,5);

(% o63) $[[0], 4, 0, 4, 0, 4, 0, 4, 0, 4]$

And those of [3]:

(% i64) padicsubstract(hensel(3/4,5,4),hensel(3/2,5,4),5);

(% o64) $[[0], 3, 3, 3, 3]$

An example on multiplication, also from [3]

(% i65) t1:hensel(4/15,5,4);

(t1) $[[-1], 3, 3, 1, 3]$

(% i66) t2:hensel(5/2,5,4);

(t2) $[[1], 3, 2, 2, 2]$

(% i67) padicmult(t1,t2,5);

(% o67) $[[0], 4, 1, 3, 1]$

Another example from [2]:

(% i68) padicmult(h1,h2,5);

(% o68) $[[1], 4, 2, 0, 1, 2, 4, 3, 2, 0]$

Example from [4]:

(% i69) al:hensel(1/4,5,4);

(al) $[[0], 4, 3, 3, 3]$

(% i70) be:hensel(1/3,5,4);

(be) $[[0], 2, 3, 1, 3]$

(% i71) padicmult(al,be,5);

(% o71) $[[0], 3, 4, 2, 4]$

The function normalhensel normalizes the Hensel code so that the first digit after the dot is not zero:

(% i72) normalhensel([[-1],0,0,1,2,3]);

(% o72) $[[1], 1, 2, 3]$

It is internally used by the function for computing divisions. Our first example is a trivial one:

(% i73) padicdiv([[0],4,0,0,0,0,0,0],[[0],2,0,0,0,0,0,0],7);

(% o73) $[[0], 2, 0, 0, 0, 0, 0, 0]$

The next example is from [2]:

(% i74) dividend:[[0],4,1,3,1,3,1,3];

(dividend) $[[0], 4, 1, 3, 1, 3, 1, 3]$

(% i75) divisor:[[0],3,4,2,4,2,4,2];

(divisor) $[[0], 3, 4, 2, 4, 2, 4, 2]$

(% i76) padicdivi(dividend,divisor,5);

(% o76) $[[0], 3, 1, 0, 0, 0, 0, 0]$

(% i77) d1:[[0],2,1,1,1];

(d1) $[[0], 2, 1, 1, 1]$

(% i78) d2:[[-1],1,1,0,0];

(d2) $[[-1], 1, 1, 0, 0]$

(% i79) padicdiv(d1,d2,5);

(% o79) $[[1], 2, 4, 1, 4]$

(% i80) padicdiv([[0],4,3,3,3],[[0],0,1,4,0],5);

(% o80) $[[-2], 0, 4, 2, 2]$

This is the example presented in [3]: 1/4/(1/2+1/3)+1/25

(% i81) padicsum(padicdiv([[0],4,3,3,3],padicsum([[0],3,2,2,2],[[0],2,3,1,3],5),5),[[-2],1,0,0,0],5);

(% o81) $[[-2], 1, 4, 2, 2]$

A quick check that the answer is correct:

(% i82) 1/4/(1/2+1/3)+1/25;

(% o82) $\frac{17}{50}$

(% i83) hensel(17/50,5,4);

(% o83) $[[-2], 1, 4, 2, 2]$

Another example, from [4]:

(% i84) alf:hensel(8/9,5,4);

(alf) $[[0], 2, 2, 4, 3]$

(% i85) bet:hensel(1/2,5,4);

(bet) $[[0], 3, 2, 2, 2]$

(% i86) padicdiv(alf,bet,5);

(% o86) $[[0], 4, 4, 3, 2]$

From [6]:

(% i87) hensel(1/333333,5,27);

(% o87) $[[0], 2, 4, 4, 4, 4, 4, 2, 1, 2, 3, 4, 4, 1, 2, 3, 1, 0, 1, 2, 3, 2, 3, 1, 3, 1, 0, 2]$

(% i88) time(%);

(% o88) $[0.001]$

Reference [6] states that 3 seconds were required for this computation, using a C++ library, in 2005.

5 From Hensel codes to rational numbers

Passing from Hensel codes to equivalent rational numbers in Q_p requires the use of the appropriate Farey fractions. A function for generating the Farey fractions I_n is farey:

(% i89) farey(17);

(% o89)

$$[0, \frac{1}{17}, \frac{1}{16}, \frac{1}{15}, \frac{1}{14}, \frac{1}{13}, \frac{1}{12}, \frac{1}{11}, \frac{1}{10}, \frac{1}{9}, \frac{2}{17}, \frac{1}{8}, \frac{2}{15}, \frac{1}{7}, \frac{2}{13}, \frac{1}{6}, \frac{3}{17}, \frac{2}{11}, \frac{3}{16}, \frac{1}{5}, \frac{3}{14}, \frac{2}{9}, \frac{3}{13}, \frac{4}{17}, \frac{1}{4}, \frac{4}{15}, \frac{3}{11}, \frac{2}{7}, \frac{5}{17}, \frac{3}{10}, \frac{4}{13},$$

(% i90) time(%);

(% o90) $[0.0]$

The package implements the algorithm by Gregory and Krishnamurthy described in the book [7]. We have added a few cases detected independently to give cleaner results. For instance, cases such as [[m],a0,0,0,0,...],[[m],a0,p-1,p-1,p-1,...] or [[m],a0,a1,...,ak,0,0,...,0s] with s>k.

Some trivial examples:

(% i91) henseltofarey([[2],3,0,0,0,0,0,0,0],7);

(% o91) 147

(% i92) henseltofarey([[0],4,4,4,4,4,4,4],5);

(% o92) -1

(% i93) henseltofarey([[0],3,3,3,3,3,3,3],5);

(% o93) $-\frac{3}{4}$

(% i94) henseltofarey([[0],0,0,0,0,0,0,0],5);

(% o94) 0

From [6] (pg 12)

(% i95) henseltofarey([[0],2,3,1,5],7);

(% o95) $$\frac{9}{43}$$

From [7] (pp. 100 and ff)

(% i96) henseltofarey([[0],0,2,4,1],5);

(% o96) $$\frac{5}{8}$$

(% i97) henseltofarey([[1],2,4,1,4],5);

(% o97) $$\frac{5}{8}$$

(% i98) henseltofarey([[-1],3,2,2,2],5);

(% o98) $$\frac{1}{10}$$

(% i99) henseltofarey([[0],3,2,2,2],5);

(% o99) $$\frac{1}{2}$$

(% i100) henseltofarey([[0],2,3,1,3],5);

(% o100) $$\frac{1}{3}$$

(% i101) henseltofarey([[0],0,6,0,6],7);

(% o101) $$-\frac{7}{8}$$

A quick check:

(% i102) hensel(1/3,5,4);

(% o102) $$[[0], 2, 3, 1, 3]$$

(%i103) hensel(-7/8,7,4);

(%o103) $[[1], 6, 0, 6, 0]$

Example from [11]:

(%i104) henseltofarey([[0],2,2,1,0],5);

(%o104) $\frac{4}{17}$

(%i105) henseltofarey([[0],1,2,1,4],5);

(%o105) $\frac{2}{7}$

Examples from the paper [8]:

(%i106) henseltofarey([[0],2,2,1,0],5);

(%o106) $\frac{4}{17}$

(%i107) henseltofarey([[0],2,2,3,4],5);

(%o107) $\frac{17}{16}$

(%i108) henseltofarey([[0],4,2,3,4],5);

(%o108) $\frac{13}{17}$

(%i109) henseltofarey([[0],1,1,0,0,1,0],3);

(%o109) $-\frac{13}{17}$

(%i110) henseltofarey([[0],1,2,1,4],5);

(%o110) $\frac{2}{7}$

(% i111) henseltofarey([[0],3,4,2,3],5);

(% o111) $\frac{11}{7}$

6 Hensel codes of square roots

Now, suppose we want to compute the square root of 2 with p=7.

We will follow [9] for that.

An integer q is called a quadratic residue mod p if there exists an

integer x such that x^2 =q mod p.

Remark: If p=2, every integer is a quadratic residue. If p is a prime

different from 2, there are (p-1)/2 residues and (p-1)/2 non-residues

in F_p-0 (that is, the multiplicative group of F_p or F^*_p).

As a consequence of the reciprocity law:

a) If p=1 mod 4, then -1 is a quadratic residue mod p.

b) I p=3 mod 4, then -1 is a non residue mod p.

Notice that every prime is equivalent to 1 or 3 mod 4.

Euler's criterion for quadratic reciprocity states that (given a in Z

and p an odd prime) the Legendre symbol evaluates to (a—p)=a^(p-1)/2.

And this equals 1 if a is a quadratic residue and -1 if it is not.

First, we introduce a function to determine whether a given integer

is a quadratic residue modulo p or not:

(% i112) sqrtmod(2,5);

(% o112)

Not a quadratic residue

Thus n=2 is not a quadratic residue modulo p=5. But it is modulo p=7:

(% i113) sqrtmod(2,7);

(% o113) $[3,4]$

If n is a quadratic residue modulo p with root x, then another root is given by the y such that y=-x mod p. We compute the padic roots with Newton's method, and the command padicsqrt –whose syntax is padicsqrt(number,p)– admits an optional argument fixing the number of iterations to be done, as in padicsqrt(number,p,iterations).

(% i114) padicsqrt(2,7);

(% o114) $$[\frac{215912063945802350977}{152672884556058511392}, \frac{2267891697076964737}{1603641597827614272}]$$

We can get the corresponding Hensel of the roots codes through

(% i115) map(lambda([u],hensel(u,7,9)),%);

(% o115) $$[[[0], 3, 1, 2, 6, 1, 2, 1, 2, 4], [[0], 4, 5, 4, 0, 5, 4, 5, 4, 2]]$$

Another example: the square root of 7 in Q_3 (from [9])

(% i116) padicsqrt(7,3,3);

(% o116) $$[\frac{977}{368}, \frac{108497}{41008}]$$

The first fraction contains 3x2=6 exact digits to determine the square root of 7 in Q_3. To get its corresponding Farey sequence it does not make sense to take more than 6 digits. Hence we do the following:

(% i117) map(lambda([u],hensel(u,3,6)),%);

(% o117) $$[[[0], 1, 1, 1, 0, 2, 0], [[0], 2, 1, 1, 2, 0, 2]]$$

(% i118) henseltofarey(%[1],3);

(% o118) $$\frac{1}{25}$$

The result is not exactly the rational we started with, but it is very close in Q_3:

(%i119) padicdist(977/368,1/25,3);

(%o119) $$\frac{1}{2187}$$

More examples:

(%i120) padicsqrt(6,5)[1];

(%o120) $$\frac{80746825394092993}{32964753427463648}$$

(%i121) hensel(%,5,4);

(%o121) $$[[0], 1, 3, 0, 4]$$

The results can be compared against those given in

http://www.numbertheory.org/php/p-adic.html

(%i122) padicsqrt(25,7);

(%o122) $$[\frac{5522138371228868332470755521}{11044276742420676262611644736}, 5]$$

(%i123) map(lambda([u],hensel(u,7,8)),%);

(%o123) $$[[[0], 2, 6, 6, 6, 6, 6, 6, 6], [[0], 5, 0, 0, 0, 0, 0, 0, 0]]$$

Example from [10]:

(%i124) padicsqrt(-2,3);

(%o124) $$[-\frac{28545857}{22783264}, \frac{28545857}{22783264}]$$

(%i125) hensel(%[1],3,8);

(%o125) $$[[0], 1, 1, 2, 0, 0, 2, 0, 1]$$

Again an example from [9], to see the influence of the choice of initial condition in Newton's iteration (notice how we fix the number of iterations as 3 here):

(% i126) padicsqrt(1,3,3);

(% o126) $$[1, \frac{3281}{3280}]$$

(% i127) map(lambda([u],hensel(u,3,8)),%);

(% o127) $$[[[0], 1, 0, 0, 0, 0, 0, 0, 0], [[0], 2, 2, 2, 2, 2, 2, 2, 2]]$$

(% i128) map(lambda([u],henseltofarey(u,3)),%);

(% o128) $$[1, -1]$$

7 Solving p-adic systems of linear equations

This is a topic of fundamental importance in applications. The algorithm implemented here is Gaussian reduction.

To solve the problem Ax=b, we have the commands padicgauss and padicbacksub. The first one triangularizes the system, and its syntax is padicgauss(B,p), where B=A—b is the augmented matrix of the system (that is, the coefficient matrix A augmented with the column b of non homogeneous terms). The resulting triangular matrix is processed by padicbacksub to obtain the Hensel codes of the solution.

The following examples are from [4]:

(% i129) D:matrix([3,1,3,16],[1,3,1,8],[1,1,3,12]);

(D) $$\begin{pmatrix} 3 & 1 & 3 & 16 \\ 1 & 3 & 1 & 8 \\ 1 & 1 & 3 & 12 \end{pmatrix}$$

(% i130) padicgauss(D,11);

(% o130) $$\begin{pmatrix} [[0], 3, 0, 0, 0] & [[0], 1, 0, 0, 0] & [[0], 3, 0, 0, 0] & [[0], 5, 1, 0, 0] \\ [[0], 0, 0, 0, 0] & [[0], 10, 3, 7, 3] & [[0], 0, 0, 0, 0] & [[0], 10, 3, 7, 3] \\ [[0], 0, 0, 0, 0] & [[0], 0, 0, 0, 0] & [[0], 2, 0, 0, 0] & [[0], 6, 0, 0, 0] \end{pmatrix}$$

(% i131) padicbacksub(%,11);

(% o131) $[[[0], 2, 0, 0, 0], [[0], 1, 0, 0, 0], [[0], 3, 0, 0, 0]]$

Converting toFarey fractions we get the rational form of the solutions:

(% i132) map(lambda([x],henseltofarey(x,11)),%);

(% o132) $[2, 1, 3]$

Another example:

(% i133) C:matrix([2,2,-1,5],[-3,0,2,-5],[4,-5,-1,0]);

(C) $$\begin{pmatrix} 2 & 2 & -1 & 5 \\ -3 & 0 & 2 & -5 \\ 4 & -5 & -1 & 0 \end{pmatrix}$$

(% i134) padicgauss(C,5);

(% o134)
$$\begin{pmatrix} [[0], 2, 0, 0, 0, 0, 0] & [[0], 2, 0, 0, 0, 0, 0] & [[0], 4, 4, 4, 4, 4, 4] & [[1], 1, 0, 0, 0, 0, 0] \\ [[0], 0, 0, 0, 0, 0, 0] & [[0], 3, 0, 0, 0, 0, 0] & [[0], 3, 2, 2, 2, 2, 2] & [[1], 3, 2, 2, 2, 2, 2] \\ [[0], 0, 0, 0, 0, 0, 0] & [[0], 0, 0, 0, 0, 0, 0] & [[0], 0, 3, 2, 2, 2, 2] & [[0], 0, 2, 2, 2, 2, 2] \end{pmatrix}$$

(% i135) padicbacksub(%,5);

(% o135) $[[[-2], 0, 0, 1, 0, 0, 0], [[-2], 0, 0, 1, 0, 0, 0], [[-2], 0, 0, 4, 4, 4, 4]]$

We convert the solution to rational (Farey) expressions:

(% i136) map(lambda([x],henseltofarey(x,5)),%);

(% o136) $[1, 1, -1]$

The examples above were trivial, the only intention was to show how the usual (rational) results are recovered within p-adic algebra. Now we consider more advanced examples, with some matrices that are highly unstable in rational arithmetic.

(%i137) E:matrix(
[10,9,8,7,6,5,4,3,2,1,1],
[9,9,8,7,6,5,4,3,2,1,2],
[8,8,8,7,6,5,4,3,2,1,-5],
[7,7,7,7,6,5,4,3,2,1,9],
[6,6,6,6,6,5,4,3,2,1,15],
[5,5,5,5,5,5,4,3,2,1,1],
[4,4,4,4,4,4,4,3,2,1,6],
[3,3,3,3,3,3,3,3,2,1,14],
[2,2,2,2,2,2,2,2,2,1,3],
[1,1,1,1,1,1,1,1,1,1,1]
);

(E) $$\begin{pmatrix} 10 & 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 & 1 \\ 9 & 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 & 2 \\ 8 & 8 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 & -5 \\ 7 & 7 & 7 & 7 & 6 & 5 & 4 & 3 & 2 & 1 & 9 \\ 6 & 6 & 6 & 6 & 6 & 5 & 4 & 3 & 2 & 1 & 15 \\ 5 & 5 & 5 & 5 & 5 & 5 & 4 & 3 & 2 & 1 & 1 \\ 4 & 4 & 4 & 4 & 4 & 4 & 4 & 3 & 2 & 1 & 6 \\ 3 & 3 & 3 & 3 & 3 & 3 & 3 & 3 & 2 & 1 & 14 \\ 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 1 & 3 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

(%i138) padicgauss(E,8209);

(%o138)
$$\begin{pmatrix} [[0],10,0,0,0,0,0,0,0] & [[0],9,0,0,0,0,0,0,0] & [[0],8,0,0,0,0,0,0,0] \\ [[0],0,0,0,0,0,0,0,0] & [[0],7389,820,7388,820,7388,820,7388,820] & [[0],6568,1641,6567,1641,6567,1641, \\ [[0],0,0,0,0,0,0,0,0] & [[0],0,0,0,0,0,0,0,0] & [[0],913,912,912,912,912,912,91 \\ [[0],0,0,0,0,0,0,0,0] & [[0],0,0,0,0,0,0,0,0] & [[0],0,0,0,0,0,0,0,0] \\ [[0],0,0,0,0,0,0,0,0] & [[0],0,0,0,0,0,0,0,0] & [[0],0,0,0,0,0,0,0,0] \\ [[0],0,0,0,0,0,0,0,0] & [[0],0,0,0,0,0,0,0,0] & [[0],0,0,0,0,0,0,0,0] \\ [[0],0,0,0,0,0,0,0,0] & [[0],0,0,0,0,0,0,0,0] & [[0],0,0,0,0,0,0,0,0] \\ [[0],0,0,0,0,0,0,0,0] & [[0],0,0,0,0,0,0,0,0] & [[0],0,0,0,0,0,0,0,0] \\ [[0],0,0,0,0,0,0,0,0] & [[0],0,0,0,0,0,0,0,0] & [[0],0,0,0,0,0,0,0,0] \\ [[0],0,0,0,0,0,0,0,0] & [[0],0,0,0,0,0,0,0,0] & [[0],0,0,0,0,0,0,0,0] \end{pmatrix}$$

(%i139) time(%);

(%o139) [1.038]

(%i140) padicbacksub(%th(2),8209);

(%o140)
[[[0], 8208, 8208, 8208, 8208, 8208, 8208, 8208, 8208], [[0], 8, 0, 0, 0, 0, 0, 0, 0], [[0], 8188, 8208, 8208, 8208, 8208, 8208,

(%i141) map(lambda([x],henseltofarey(x,8209)),%);

(%o141) $[-1, 8, -21, 8, 20, -19, -3, 19, -9, -1]$

Hibert matrices are known for their bad condition number. This is a good opportunity to appreciate the advantages of working with p-adics:

(%i142) F:addcol(hilbert_matrix(5),[137/60,87/60,459/420,743/840,1875/2520]);

(F) $$\begin{pmatrix} 1 & \frac{1}{2} & \frac{1}{3} & \frac{1}{4} & \frac{1}{5} & \frac{137}{60} \\ \frac{1}{2} & \frac{1}{3} & \frac{1}{4} & \frac{1}{5} & \frac{1}{6} & \frac{29}{20} \\ \frac{1}{3} & \frac{1}{4} & \frac{1}{5} & \frac{1}{6} & \frac{1}{7} & \frac{153}{140} \\ \frac{1}{4} & \frac{1}{5} & \frac{1}{6} & \frac{1}{7} & \frac{1}{8} & \frac{743}{840} \\ \frac{1}{5} & \frac{1}{6} & \frac{1}{7} & \frac{1}{8} & \frac{1}{9} & \frac{125}{168} \end{pmatrix}$$

(%i143) padicgauss(F,8209);

(%o143)

[[0], 1, 0, 0, 0, 0, 0, 0, 0]	[[0], 4105, 4104, 4104, 4104, 4104, 4104, 4104, 4104]	[[0], 5473, 5472, 5472, 5472, 5472, 54
[[0], 0, 0, 0, 0, 0, 0, 0, 0]	[[0], 7525, 7524, 7524, 7524, 7524, 7524, 7524, 7524]	[[0], 7525, 7524, 7524, 7524, 7524, 75
[[0], 0, 0, 0, 0, 0, 0, 0, 0]	[[0], 0, 0, 0, 0, 0, 0, 0, 0]	[[0], 3238, 8163, 3237, 8163, 3237, 81
[[0], 0, 0, 0, 0, 0, 0, 0, 0]	[[0], 0, 0, 0, 0, 0, 0, 0, 0]	[[0], 0, 0, 0, 0, 0, 0, 0, 0
[[0], 0, 0, 0, 0, 0, 0, 0, 0]	[[0], 0, 0, 0, 0, 0, 0, 0, 0]	[[0], 0, 0, 0, 0, 0, 0, 0, 0

(%i144) time(%);

(%o144) [0.161]

(%i145) padicbacksub(%th(2),8209);

(%o145)
[[[0], 0, 0, 0, 0, 0, 0, 0, 0], [[0], 21, 0, 0, 0, 0, 0, 0, 0], [[0], 8120, 8208, 8208, 8208, 8208, 8208, 8208, 8208], [[0], 141, 0, 0, 0,

(%i146) map(lambda([x],henseltofarey(x,8209)),%);

(%o146) $[0, 21, -89, 141, -69]$

There will be a lot of situatons where our simple heuristis for choosing t will lead to bad values. For those cases, one can manually choose t using the alternative function padicgauss2. Below we choose 8 digits:

(%i147) padicgauss2(E,8209,8);

(%o147)

$$\begin{pmatrix} [[0],10,0,0,0,0,0,0,0] & [[0],9,0,0,0,0,0,0,0] & [[0],8,0,0,0,0,0,0,0] \\ [[0],0,0,0,0,0,0,0,0] & [[0],7389,820,7388,820,7388,820,7388,820] & [[0],6568,1641,6567,1641,6567,1641, \\ [[0],0,0,0,0,0,0,0,0] & [[0],0,0,0,0,0,0,0,0] & [[0],913,912,912,912,912,912,91 \\ [[0],0,0,0,0,0,0,0,0] & [[0],0,0,0,0,0,0,0,0] & [[0],0,0,0,0,0,0,0,0] \\ [[0],0,0,0,0,0,0,0,0] & [[0],0,0,0,0,0,0,0,0] & [[0],0,0,0,0,0,0,0,0] \\ [[0],0,0,0,0,0,0,0,0] & [[0],0,0,0,0,0,0,0,0] & [[0],0,0,0,0,0,0,0,0] \\ [[0],0,0,0,0,0,0,0,0] & [[0],0,0,0,0,0,0,0,0] & [[0],0,0,0,0,0,0,0,0] \\ [[0],0,0,0,0,0,0,0,0] & [[0],0,0,0,0,0,0,0,0] & [[0],0,0,0,0,0,0,0,0] \\ [[0],0,0,0,0,0,0,0,0] & [[0],0,0,0,0,0,0,0,0] & [[0],0,0,0,0,0,0,0,0] \\ [[0],0,0,0,0,0,0,0,0] & [[0],0,0,0,0,0,0,0,0] & [[0],0,0,0,0,0,0,0,0] \end{pmatrix}$$

(%i148) padicbacksub(%,8209);

(%o148)

$[[[0],8208,8208,8208,8208,8208,8208,8208,8208],[[0],8,0,0,0,0,0,0,0],[[0],8188,8208,8208,8208,8208,8208,$

(%i149) map(lambda([x],henseltofarey(x,8209)),%);

(%o149) $[-1, 8, -21, 8, 20, -19, -3, 19, -9, -1]$

Let us see how p-adic arithmetics deal with the high condition number of Hilbert matrices and the associated instabilities:

(%i150) M1:addcol(hilbert_matrix(5),makelist(j,j,1,5));

(M1) $$\begin{pmatrix} 1 & \frac{1}{2} & \frac{1}{3} & \frac{1}{4} & \frac{1}{5} & 1 \\ \frac{1}{2} & \frac{1}{3} & \frac{1}{4} & \frac{1}{5} & \frac{1}{6} & 2 \\ \frac{1}{3} & \frac{1}{4} & \frac{1}{5} & \frac{1}{6} & \frac{1}{7} & 3 \\ \frac{1}{4} & \frac{1}{5} & \frac{1}{6} & \frac{1}{7} & \frac{1}{8} & 4 \\ \frac{1}{5} & \frac{1}{6} & \frac{1}{7} & \frac{1}{8} & \frac{1}{9} & 5 \end{pmatrix}$$

(%i151) M2:addcol(hilbert_matrix(5),makelist(j+29^(3+random(6)),j,1,5));

$$(M2)\quad \begin{pmatrix} 1 & \frac{1}{2} & \frac{1}{3} & \frac{1}{4} & \frac{1}{5} & 20511150 \\ \frac{1}{2} & \frac{1}{3} & \frac{1}{4} & \frac{1}{5} & \frac{1}{6} & 24391 \\ \frac{1}{3} & \frac{1}{4} & \frac{1}{5} & \frac{1}{6} & \frac{1}{7} & 20511152 \\ \frac{1}{4} & \frac{1}{5} & \frac{1}{6} & \frac{1}{7} & \frac{1}{8} & 500246412965 \\ \frac{1}{5} & \frac{1}{6} & \frac{1}{7} & \frac{1}{8} & \frac{1}{9} & 17249876314 \end{pmatrix}$$

Notice that the non-homogeneous coefficients in M2 are really close to the initial ones in M1:

(%i152) makelist(padicdist(M1[j][6],M2[j][6],29),j,1,length(M1));

$$(\%o152)\quad [\frac{1}{20511149}, \frac{1}{24389}, \frac{1}{20511149}, \frac{1}{500246412961}, \frac{1}{17249876309}]$$

(%i153) padicgauss2(M1,29,6);

(%o153)

$$\begin{pmatrix} [[0],1,0,0,0,0,0] & [[0],15,14,14,14,14,14] & [[0],10,19,9,19,9,19] & [[0],22,21,21,21,21,21] & [[0],6,23, \\ [[0],0,0,0,0,0,0] & [[0],17,26,16,26,16,26] & [[0],17,26,16,26,16,26] & [[0],24,26,23,26,23,26] & [[0],2,27, \\ [[0],0,0,0,0,0,0] & [[0],0,0,0,0,0,0] & [[0],5,19,14,9,24,28] & [[0],22,28,21,28,21,28] & [[0],21,28,2 \\ [[0],0,0,0,0,0,0] & [[0],0,0,0,0,0,0] & [[0],0,0,0,0,0,0] & [[0],20,8,11,17,2,26] & [[0],11,17, \\ [[0],0,0,0,0,0,0] & [[0],0,0,0,0,0,0] & [[0],0,0,0,0,0,0] & [[0],0,0,0,0,0,0] & [[0],16,0, \end{pmatrix}$$

(%i154) padicbacksub(%,29);

(%o154)

$$[[[0],9,4,0,0,0,0],[[0],20,16,25,28,28,28],[[0],19,6,17,0,0,0],[[0],10,20,28,27,28,28],[[0],6,21,15,0,0,0]]$$

(%i155) map(lambda([x],henseltofarey(x,29)),%);

$$(\%o155)\quad [125, -2880, 14490, \frac{1}{47339632}, 13230]$$

(%i156) padicgauss2(M2,29,6);

(%o156)

$$\begin{pmatrix} [[0],1,0,0,0,0,0] & [[0],15,14,14,14,14,14] & [[0],10,19,9,19,9,19] & [[0],22,21,21,21,21,21] & [[0],6,23, \\ [[0],0,0,0,0,0,0] & [[0],17,26,16,26,16,26] & [[0],17,26,16,26,16,26] & [[0],24,26,23,26,23,26] & [[0],2,27, \\ [[0],0,0,0,0,0,0] & [[0],0,0,0,0,0,0] & [[0],5,19,14,9,24,28] & [[0],22,28,21,28,21,28] & [[0],21,28,2 \\ [[0],0,0,0,0,0,0] & [[0],0,0,0,0,0,0] & [[0],0,0,0,0,0,0] & [[0],20,8,11,17,2,26] & [[0],11,17, \\ [[0],0,0,0,0,0,0] & [[0],0,0,0,0,0,0] & [[0],0,0,0,0,0,0] & [[0],0,0,0,0,0,0] & [[0],16,0, \end{pmatrix}$$

(% i157) padicbacksub(%,29);

(% o157)
$[[[0],9,4,0,19,18,1],[[0],20,16,25,14,20,3],[[0],19,6,17,8,15,19],[[0],10,20,28,24,27,18],[[0],6,21,15,15,0,1$

(% i158) map(lambda([x],henseltofarey(x,29)),%);

(% o158) $$[\frac{1}{73774969},\frac{2}{122364169},-\frac{4725}{9013},\frac{1}{83362185},\frac{2}{80199829}]$$

The solutions of the original system and the perturbed one, are quite close (in the p-adic distance, of course):

(% i159) makelist(padicdist(%[j],%th(4)[j],29),j,1,length(%));

(% o159) $$[\frac{1}{24389},\frac{1}{24389},\frac{1}{24389},\frac{1}{24389},\frac{1}{24389}]$$

For comparison, let us see how things work in the purely rational case:

(% i160) A:hilbert_matrix(5)$

(% i161) X:makelist(x[k],k,1,5)$

(% i162) B1:makelist(k,k,1,5)$

(% i163) B2:makelist(rat(k+random(0.01)),k,1,5)$

(% i164) for j:1 thru 5 do eq1[j]:sum(A[j,k]*X[k],k,1,5)=B1[j]$

(% i165) for j:1 thru 5 do eq2[j]:sum(A[j,k]*X[k],k,1,5)=B2[j]$

(% i166) solve(makelist(eq1[j],j,1,5),X);

(% o166) $$[[x_1=125,x_2=-2880,x_3=14490,x_4=-24640,x_5=13230]]$$

(% i167) solve(makelist(eq2[j],j,1,5),X),numer;

(% o167)

$[[x_1 = 120.1003883272046, x_2 = -2780.48089521768, x_3 = 14040.16509590324, x_4 = -23939.74158066582, x_5 =$

Those solutions are far away from each other in the usual absolute value distance. This example is a striking evidence of the better stability properties of p-adic arithmetic over the traditional rational one.

8 References

[1] G. Bachman: Introduction to p–adic Numbers and Valuation Theory, Academic Press, New York, NY, 1964.

[2] C. K. Koc: A Tutorial on p-adic Arithmetic. Oregon State University. Technical Report, April 2002. Available at http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.81.2931&rep=rep1&type=pdf

[3] C. Limongelli and R. Pirastu: p-adic Arithmetic and Parallel Symbolic Computation: An Implementation for Solving Linear Systems. Computers and Artificial Intelligence 14 n. 1 (1996) 35-62.

[4] E. V. Krishnamurty, T. Mahadeva Rao and K. Subramanian: p-Adic arithmetic procedures for exact matrix computations. Proc, Indian Acad. Sci., Vol. 82A, No. 5 (1975) 165-175.

[5] C. Limongelli: On an efficient algorithm for big rational number computations by parallel p-adics. J. Symbolic Computation 15 (1993) 181-197.

[6] C. Lu: A Computational Library Using p-adic Arithmetic for Exact Computation With Rational Numbers in Quantum Computing. Final Report (Grant ≠FA9550-05-1-0363) Towson University, 2005.

[7] R. T. Gregory and E. V. Krishnamurthy: Methods and Applications of Error-Free Computation. Springer Verlag, 1984.

[8] V. E. Krishnamurthy : On the Conversion of Hensel Codes to Farey Rationals. IEEE Transactions on computers, vol c-32, No. 4, April 1983

[9] K. Conrad: Hensel's Lemma. Available at

https://kconrad.math.uconn.edu/blurbs/gradnumthy/hensel.pdf

[10] J. E. Cremona: Introduction to Number Theory Lecture Notes, 2018. Available at
http://homepages.warwick.ac.uk/staff/J.E.Cremona/courses/MA257/ma257.pdf

[11] A. Vimawala: p-Adic Arithmetic Methods for Exact Computations of Rational Numbers. School of Electrical Engineering and Computer Science, Oregon State University. Available at:
http://cs.ucsb.edu/koc/cs290g/project/2003/vimawala.pdf