A Tutorial on p-adic Arithmetic

Ç. K. Koç
Electrical & Computer Engineering
Oregon State University
Corvallis, Oregon 97331

Technical Report, April 2002

Abstract

The p-adic arithmetic allows error-free representation of fractions and error-free arithmetic using fractions. In this tutorial, we describe infinite-precision p-adic arithmetic which is more suitable for software implementations and finite-precision p-adic arithmetic which is more suitable for hardware implementations. The finite-precision p-adic representation is also called Hensel code which has certain interesting properties and some open problems for research.

1 Introduction

A p-adic number α can be uniquely written in the form

$$\alpha = \sum_{j=n}^{\infty} a_j p^j$$

where each of $a_j \in [0, p-1]$ and the p-adic norm of the number α is defined as $\| \alpha \| = p^{-n}$. Note that the series

$$1 + p + p^2 + p^3 + \cdots$$

converges to $\frac{1}{1-p}$ in the p-adic norm. Now, as an example, consider the power series expansion

$$\begin{aligned} \alpha &= 2 + 3p + p^2 + 3p^3 + p^4 + 3p^5 + p^6 + \cdots \\ &= 2 + 3p(1 + p^2 + p^4 + \cdots) + p^2(1 + p^2 + p^4 + \cdots) \\ &= 2 + (3p + p^2)(1 + p^2 + p^4 + \cdots) \end{aligned}$$

Since $1 + p^2 + p^4 + \cdots$ converges to $(1 - p^2)^{-1}$, we have

$$\alpha = 2 + \frac{3p + p^2}{1 - p^2} \ .$$

Taking $p = 5$, we obtain 5-adic expansion of $\alpha = \frac{1}{3}$, which can be written in the form

$$\begin{aligned} \frac{1}{3} &= .23131313131\cdots \quad (p = 5) \\ &= .2\overline{31} \quad (p = 5) \ . \end{aligned}$$

There is a one-to-one correspondence between the power series expansion

$$a_n p^n + a_{n+1} p^{n+1} + a_{n+2} p^{n+2} + \cdots$$

and the short representation $a_n a_{n+1} a_{n+2} \cdots$, where only the coefficients of the powers of p are shown. We can use the p-adic point as a device for displaying the sign of n.

$$\begin{array}{rl} a_n a_{n+1} \cdots a_{-2} a_{-1} . a_0 a_1 a_2 \cdots & \text{for } n < 0 \\ . a_0 a_1 a_2 \cdots & \text{for } n = 0 \\ .00 \cdots 0 a_0 a_1 a_2 \cdots & \text{for } n > 0 \end{array}$$

For example,

$$\begin{array}{rcrcl} 13.41 & = & 1 \cdot 5^{-2} + 3 \cdot 5^{-1} + 4 \cdot 5^0 + 1 \cdot 5^1 & = & 241/25 \\ .1341 & = & 1 \cdot 5^0 + 3 \cdot 5^1 + 4 \cdot 5^2 + 1 \cdot 5^3 & = & 241 \\ .01341 & = & 0 \cdot 5^0 + 1 \cdot 5^1 + 3 \cdot 5^2 + 4 \cdot 5^3 + 1 \cdot 5^4 & = & 1205 \end{array}$$

2 Representation of Negative Numbers

If

$$\alpha = \sum_{i=n}^{\infty} a_i p^i$$

then

$$-\alpha = \sum_{i=n}^{\infty} b_i p^i$$

where $b_n = p - a_n$ and $b_i = (p-1) - a_i$ for $i > n$. Thus, for example,

$$\begin{array}{rcl} \frac{1}{3} & = & .2313131 \cdots \\ -\frac{1}{3} & = & .3131313 \cdots \end{array}$$

However, watch for leading zeros, they remain unchanged:

$$\begin{array}{rcl} \frac{5}{3} & = & .02313131 \cdots \\ -\frac{5}{3} & = & .03131313 \cdots \end{array}$$

3 Representation of Integers

Since a positive integer h can be expressed in exactly one way as the sum of powers of a prime p, i.e.,

$$h = d_0 + d_1 p + d_2 p^2 + \cdots + d_k p^k$$

with $d_i \in [0, p-1]$, there is essentially no difference between p-adic and p-ary representation of h. The only difference is that the digits in the p-adic representation are written in reverse order. For example,

$$\begin{array}{rcrcll} 199 & = & 4 \cdot 5^0 + 4 \cdot 5^1 + 2 \cdot 5^2 + 1 \cdot 5^3 & = & .4421 & \text{(5-adic)} \\ 199 & = & 1 \cdot 5^3 + 2 \cdot 5^2 + 4 \cdot 5^1 + 4 \cdot 5^0 & = & 1244. & \text{(5-ary)} \end{array}$$

4 Representation of Rational Numbers

If α is a rational number, then it has a repeating pattern of a_js in its p-adic expansion, i.e., it is of the form

$$\alpha = a_n a_{n+1} \cdots a_{-1} . b_0 b_1 \cdots b_k \overline{c_1 c_2 \cdots c_l}$$

For example, $1/3 = .2\overline{31}$, $-1/3 = .\overline{31}$, and $2/3 = .4\overline{13}$, etc. Let α have the p-adic expansion

$$\begin{aligned} \alpha &= a_n p^n + a_{n+1} p^{n+1} + a_{n+2} p^{n+2} + \cdots \\ &= p^n (a_n + a_{n+1} p + a_{n+2} p^2 + \cdots) \\ &= p^n \cdot \frac{c_1}{d_1} \end{aligned}$$

where $\gcd(c_1, d_1) = 1$ and p divides neither c_1 nor d_1. The p-adic expansion for c_1/d_1 is

$$\frac{c_1}{d_1} = a_n + a_{n+1} p + a_{n+2} p^2 + \cdots$$

and thus

$$\begin{aligned} c_1 \cdot d_1^{-1} \pmod{p} &= a_n + a_{n+1} p + a_{n+2} p^2 + \cdots \pmod{p} \\ &= a_n \ . \end{aligned}$$

In other words, we compute a_n by

$$a_n = c_1 \cdot d_1^{-1} \pmod{p} \ .$$

Next, we use

$$\begin{aligned} \frac{c_1}{d_1} - a_n &= p(a_{n+1} + a_{n+2} p + a_{n+3} p^2 + \cdots) \\ &= p \cdot \frac{c_2}{d_2} \ , \end{aligned}$$

where $\gcd(c_2, d_2) = 1$ and p divides neither c_2 nor d_2. The p-adic expansion for c_2/d_2 is

$$\frac{c_2}{d_2} = a_{n+1} + a_{n+2} p + a_{n+3} p^2 + \cdots$$

and so

$$a_{n+1} = c_2 \cdot d_2^{-1} \pmod{p} \ .$$

We continue this process until the period is exhibited. Let $\alpha = 2/15$ and $p = 5$. Thus,

$$\frac{2}{15} = 5^{-1} \cdot \frac{2}{3} \ ,$$

and $n = -1$. The 5-adic expansion of $2/15$ is found as

$$\begin{aligned} a_{-1} &= 2 \cdot 3^{-1} \pmod{5} \ = \ 4 \\ \frac{2}{3} - 4 &= -\frac{10}{3} = 5 \cdot \frac{-2}{3} \\ a_0 &= -2 \cdot 3^{-1} \pmod{5} \ = \ 1 \end{aligned}$$

$$
\begin{aligned}
\frac{-2}{3} - 1 &= -\frac{5}{3} = 5 \cdot \frac{-1}{3} \\
a_1 &= -1 \cdot 3^{-1} \pmod 5 = 3 \\
\frac{-1}{3} - 3 &= -\frac{10}{3} = 5 \cdot \frac{-2}{3} \\
a_2 &= -2 \cdot 3^{-1} \pmod 5 = 1 \\
\frac{-2}{3} - 1 &= -\frac{5}{3} = 5 \cdot \frac{-1}{3} \\
a_3 &= -1 \cdot 3^{-1} \pmod 5 = 3
\end{aligned}
$$

which gives us $2/15 = 4.131313\cdots = 4.\overline{13}$.

5 Addition

Addition of p-adic numbers is similar to the addition of p-ary numbers. However, we add the digits and propagate the carries from left to right. As an example, we compute $2/3 + 5/6 = 3/2$ for $p = 5$.

$$
\begin{aligned}
\frac{2}{3} &= .413131313\cdots \\
\frac{5}{6} &= .014040404\cdots
\end{aligned}
$$

The addition operation proceeds as follows:

$$
\begin{array}{rcl}
.413131313\cdots & = & .4\overline{13} \\
.014040404\cdots & = & .01\overline{40} \\
\hline
.422222222\cdots & = & .4\overline{2}
\end{array}
$$

As a check, we convert $.4\overline{2}$ to rational

$$
\begin{aligned}
.4\overline{2} &= 4 + 2(5 + 5^2 + 5^3 + \cdots) \\
&= 4 + 10(1 + 5 + 5^2 + 5^3 + \cdots) \\
&= 4 + 10 \cdot \frac{1}{1-5} \\
&= \frac{3}{2}\,.
\end{aligned}
$$

6 Subtraction

We complement the subtrahend and add it to the minuend, i.e., $\alpha - \beta = \alpha + (-\beta)$. Let $\alpha = 2/3$ and $\beta = 5/6$, then

$$
\begin{aligned}
\frac{5}{6} &= .014040404\cdots \\
-\frac{5}{6} &= .040404040\cdots
\end{aligned}
$$

Thus, we compute $2/3 - 5/6 = -1/6$ as

$$\begin{array}{rcl} .413131313\cdots & = & .4\overline{13} \\ .040404040\cdots & = & .\overline{04} \\ \hline .404040404\cdots & = & .\overline{40} \end{array}$$

Now, we convert $.\overline{40}$ to rational using

$$\begin{aligned} .\overline{40} &= 4(1+5^2+5^4+5^6+\cdots) \\ &= 4\cdot\frac{1}{1-25} \\ &= -\frac{1}{6}\,. \end{aligned}$$

7 Multiplication

A p-adic number is called unit if it is not a multiple of a negative power of p and its first digit is nonzero. For example, $.4\overline{13}$ and $.4\overline{2}$ are units while $.01\overline{40}$ and $42.12\overline{31}$ are not. A non-unit p-adic number α can always be written in the form $\alpha = \gamma \cdot p^n$ where γ is a unit. For example,

$$.01\overline{40} = .1\overline{40}\cdot 5^1$$

and

$$42.12\overline{31} = .4212\overline{31}\cdot 5^{-2}\,.$$

Let $\alpha = p^n\gamma$ and $\beta = p^m\theta$, then $\alpha\beta = p^{n+m}\gamma\theta$. We can thus restrict multiplication of any two p-adic numbers to multiplication of units. The multiplication can then be carried similar to the case of p-ary numbers. To multiply 2/3 and 5/6, we get the Hensel codes‘

$$\begin{aligned} \frac{2}{3} &= .413131313\cdots \\ \frac{1}{6} &= .140404040\cdots \end{aligned}$$

The multiplication operation is illustrated below:

$$\begin{array}{rr} & .4131313131313\cdots \\ \times & .1404040404040\cdots \\ \hline & 4131313131313\cdots \\ & 123131313131\cdots \\ & 00000000000\cdots \\ & 1231313131\cdots \\ & 000000000\cdots \\ & 12313131\cdots \\ & 0000000\cdots \\ & 123131\cdots \\ & 00000\cdots \\ & 1231\cdots \\ & 000\cdots \\ & 12\cdots \\ + & 0\cdots \\ \hline & .4201243201243\cdots \end{array}$$

Thus, the result is $0.4\overline{201243}$ which is equal to

$$\frac{2}{3} \cdot \frac{1}{6} = \frac{1}{9} \ .$$

8 Division

Again, we will only consider the division of p-adic units. Consider the following p-adic units:

$$\begin{aligned} \delta &= d_0 + d_1 p + d_2 p^2 + \cdots \\ \beta &= b_0 + b_1 p + b_2 p^2 + \cdots \end{aligned}$$

with $d_0, b_0 \neq 0$. The quotient $\alpha = \delta/\beta$ can be written

$$\begin{aligned} \alpha &= \frac{d_0 + d_1 p + d_2 p^2 + \cdots}{b_0 + b_1 p + b_2 p^2 + \cdots} \\ &= a_0 + a_1 p + a_2 p^2 + \cdots \end{aligned}$$

where $a_0, a_1, a_1, \ldots$ are the digits of α. Since $\delta = \beta \cdot \alpha$, we have

$$\begin{aligned} \beta \cdot \alpha &= (b_0 + b_1 p + b_2 p^2 + \cdots)(a_0 + a_1 p + a_2 p^2 + \cdots) \\ &= c_0 + c_1 p + c_2 p^2 + \cdots \end{aligned}$$

Even though the p-adic digits a_i and b_i lie in the interval $[0, p-1]$, we cannot assume that the integers c_i lie in this interval. Hence we write

$$c_0 = b_0 a_0 = d_0 + t_1 p$$

where $d_0 \in [0, p-1]$. Then d_0 is the first digit in the p-adic expansion for $\beta\alpha$ and t_1 is the *carry* which must be added to c_1. Thus,

$$d_0 = a_0 b_0 \pmod{p}$$

which implies

$$a_0 = d_0 b_0^{-1} \pmod{p} \ .$$

This turns out to be the rule for obtaining each digit of the expansion for α. At each stage of the standard *long division* procedure, we multiply $b_0^{-1} \pmod{p}$ by the first digit of the partial remainder and reduce the result modulo p.

As an example, we divide 2/3 by 1/12. We have

$$\begin{aligned} \frac{2}{3} &= .4131313\cdots \\ \frac{1}{12} &= .3424242\cdots \end{aligned}$$

The first digit of the divisor is $b_0 = 3$ and its multiplicative inverse modulo 5 is

$$\begin{aligned} b_0^{-1} \pmod{p} &= 3^{-1} \pmod{5} \\ &= 2 \ . \end{aligned}$$

The first digit of the partial remainder (which, in the first step, is the dividend) is $d_0 = 4$, which gives

$$\begin{aligned} a_0 &= b_0^{-1} d_0 \pmod{p} \\ &= 2 \cdot 4 \pmod{5} \\ &= 3 \ . \end{aligned}$$

Thus, we obtain the first digit of the quotient. We then update the partial remainder by subtracting 3 times the divisor from it.

$$\begin{array}{rr} & .3 \\ \hline .3424242\cdots & .4131313\cdots \\ .4333333\cdots & .1111111\cdots \\ \hline & .0342424\cdots \end{array}$$

To obtain the second digit, we multiply $b_0^{-1} \pmod{p}$ by the first digit of the partial remainder and reduce the result modulo p.

$$\begin{aligned} a_1 &= 2 \cdot 3 \pmod{5} \\ &= 1 \ . \end{aligned}$$

Thus, the second step of the division procedure gives us

$$\begin{array}{rr} & .31 \\ \hline .3424242\cdots & .0342424\cdots \\ .0342424\cdots & .0202020\cdots \\ \hline & .0000000\cdots \end{array}$$

This procedure produced the partial remainder which is zero, hence we terminate the expansion. In general, this will not happen and we will have to continue until the period is exhibited. As a check we observe that $2/3 \div 1/12 = 8$ and $8 = .31$ for $p = 5$.

We note that the division of p-adic numbers is deterministic and not subject to trial and error as is the case for division of p-ary numbers.

9 Finite-Segment p-adic Number System

In this finite number system each rational number in the set

$$S_N = \{\alpha = \frac{a}{b} \ : \ |a| \in [0, N], \text{ and } |b| \in [1, N]\}$$

is assigned a unique code representation called its *Hensel code*. Arithmetic operations on pairs of rational numbers in S_N can be replaced by corresponding arithmetic operations on their Hensel codes.

A Hensel code for a rational number α is simply a finite segment of its infinite-precision p-adic expansion. We use the notation $H(p, r, \alpha)$ where p is a prime and r is the integer which specifies the number of digits of the p-adic expansion which we retain for the Hensel code. For example, since

$$\frac{2}{3} = 0.4131313\cdots \ ,$$

the Hensel code for $\alpha = 2/3$ when $p = 5$ and $r = 4$ is

$$H(5, 4, 2/3) = .4131 \ .$$

A Farey sequence of order N is the ascending sequence of all reduced fractions in $[0, 1]$ whose denominators are not greater than N. For example, if $N = 5$, we have the Farey sequence

$$F_5 = \frac{0}{1}, \frac{1}{5}, \frac{1}{4}, \frac{1}{3}, \frac{2}{5}, \frac{1}{2}, \frac{3}{5}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5}, \frac{1}{1} \ .$$

A simple rule for obtaining the Farey sequence of any order is illustrated below:

$$\begin{array}{lccccccccccc}
F_1: & \frac{0}{1} & & & & & & & & & & \frac{1}{1} \\
F_2: & \frac{0}{1} & & & & & \frac{1}{2} & & & & & \frac{1}{1} \\
F_3: & \frac{0}{1} & & & \frac{1}{3} & & \frac{1}{2} & & \frac{2}{3} & & & \frac{1}{1} \\
F_4: & \frac{0}{1} & & \frac{1}{4} & \frac{1}{3} & & \frac{1}{2} & & \frac{2}{3} & \frac{3}{4} & & \frac{1}{1} \\
F_5: & \frac{0}{1} & \frac{1}{5} & \frac{1}{4} & \frac{1}{3} & \frac{2}{5} & \frac{1}{2} & \frac{3}{5} & \frac{2}{3} & \frac{3}{4} & \frac{4}{5} & \frac{1}{1}
\end{array}$$

where the nth row is constructed from the $(n-1)$st row by including the fraction $\frac{a+b}{c+d}$ between any two fractions $\frac{a}{c}$ and $\frac{b}{d}$ whenever $c + d \leq n$. Note that the set S_N is the set of all order N Farey fractions.

Theorem 1 *Let p be a prime and let r be a positive integer. Define N to be the largest positive integer which satisfies the inequality*

$$N \leq \left(\frac{p^r - 1}{2}\right)^{\frac{1}{2}}$$

then every order N Farey fraction α can be represented uniquely by an r-digit ordered sequence (its Hensel code), where each digit is an integer in the interval $[0, p-1]$.

For example, for $p = 5$ and $r = 4$, the value of N is found by computing

$$N \leq \left(\frac{5^4 - 1}{2}\right)^{\frac{1}{2}} \ ,$$

which gives $N = 17$. Thus, if a/b belongs to F_{17}, we have a unique Hensel code $H(5, 4, a/b)$ for it.

We do not have compute infinite p-adic expansion of α in order to obtain r-digit Hensel code of α. Suppose $\alpha = \frac{a}{b}$ where

$$\frac{a}{b} = p^n \cdot \frac{c}{d}$$

with $\gcd(c, d) = \gcd(c, p) = \gcd(d, p) = 1$. Let the Hensel code for c/d be

$$H(p, r, c/d) = .a_0 a_1 \cdots a_{r-1}$$

then $a_{r-1} a_{r-2} \cdots a_1 a_0$ is the radix p representation for the integer $c \cdot d^{-1} \pmod{p^r}$, i.e.,

$$a_0 + a_1 p + a_2 p^2 + \cdots + a_{r-1} p^{r-1} = c \cdot d^{-1} \pmod{p^r} \ .$$

We consider the following three cases:

Case I $n = 0$

First we compute the integer $c \cdot d^{-1} \pmod{p^r}$ and then express this integer in radix p. The Hensel code is then simply obtained by reversing the digits. For example, when $\alpha = 2/3$, $p = 5$, and $r = 4$, we have $p^r = 5^4 = 625$, and

$$\frac{2}{3} = 5^0 \cdot \frac{2}{3} \ ,$$

thus

$$2 \cdot 3^{-1} = 2 \cdot 417 = 209 \pmod{625} \ .$$

Expressing the decimal 209 in radix 5, we obtain

$$209 = 1 \cdot 5^3 + 3 \cdot 5^2 + 1 \cdot 5^1 + 4 \cdot 5^0 = (1314)_5 \ .$$

The Hensel code of 2/3 is found

$$H(5, 4, 2/3) = .4131$$

which agrees with the one found by truncating the infinite series expansion.

Case II $n < 0$

In this case $\alpha = p^{-m} \cdot \frac{c}{d}$ where m is a positive integer. To find $H(p, r, \alpha)$ we first find $H(p, r, c/d)$ using the procedure given in Case I and then shift the p-adic point m places to the right. For example, let $\alpha = 2/15$ with $p = 5$ and $r = 4$. We write $\alpha = 5^{-1} \cdot \frac{2}{3}$ and compute the Hensel code for 2/3 as .4131. The Hensel code for 2/15 is found by shifting the p-adic point one place to the right to obtain

$$H(5, 4, 2/15) = 4.131$$

Case III $n > 0$

In this case $\alpha = p^k \cdot \frac{c}{d}$ where k is a positive integer. To find $H(p, r, \alpha)$ we compute $H(p, r, c/d)$ and then shift the p-adic point k places to the left. For example, the Hensel code $\alpha = 10/3 = 5^1 \cdot \frac{2}{3}$ is found as

$$H(5, 4, 10/3) = .0413$$

Note that the rules for obtaining Hensel code for a negative number are the same. For example, to obtain $H(5, 4, -2/3)$ we compute 5-ary expansion of the integer $-2 \cdot 3^{-1} \pmod{625}$ as

$$\begin{aligned} &= -2 \cdot 3^{-1} \pmod{625} \\ &= -2 \cdot 417 \pmod{625} \\ &= 416 \\ &= (3131)_5 \end{aligned}$$

which gives the Hensel code $H(5, 4, -2/3) = .1313$.

10 Arithmetic using Hensel Codes

The rules of the arithmetic are similar to the infinite-precision case. However, notice that whenever the result is outside the set F_N, uniqueness and correctness are no longer assured. The table given below enumerates all Hensel codes of the form $H(5, 4, a/b)$ where $a/b \in F_{17}$.

Table 1: Ordinary Hensel Codes $H(5, 4, a/b)$

a b	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
1	.1000	.3222	.2313	.4333	1.000	.1404	.3302	.2414	.4201	3.222	.1332	.3424	.2034	.4101	2.313	.1234	.3043
2	.2000	.1000	.4131	.3222	2.000	.2313	.1214	.4333	.3012	1.000	.2120	.1404	.4014	.3302	4.131	.2414	.1132
3	.3000	.4222	.1000	.2111	3.000	.3222	.4021	.1303	.2313	4.222	.3403	.4333	.1143	.2013	1.000	.3104	.4121
4	.4000	.2000	.3313	.1000	4.000	.4131	.2423	.3222	.1124	2.000	.4240	.2313	.3123	.1214	3.313	.4333	.2210
5	.0100	.0322	.0231	.0433	.1000	.0140	.0330	.0241	.0420	.3222	.0133	.0342	.0203	.0410	.2313	.0123	.0304
6	.1100	.3000	.2000	.4222	1.100	.1000	.3142	.2111	.4131	3.000	.1411	.3222	.2232	.4021	2.000	.1303	.3342
7	.2100	.1322	.4313	.3111	2.100	.2404	.1000	.4030	.3432	1.322	.2204	.1202	.4212	.3222	4.313	.2042	.1431
8	.3100	.4000	.1231	.2000	3.100	.3313	.4302	.1000	.2243	4.000	.3041	.4131	.1341	.2423	1.231	.3222	.4420
9	.4100	.2322	.3000	.1433	4.100	.4222	.2214	.3414	.1000	2.322	.4324	.2111	.3321	.1134	3.000	.4402	.2024
10	.0200	.0100	.0413	.0322	.2000	.0231	.0121	.0433	.0301	.1000	.0212	.0140	.0401	.0330	.4131	.0241	.0113
11	.1200	.3322	.2231	.4111	1.200	.1140	.3423	.2303	.4012	3.322	.1000	.3020	.2430	.4431	2.231	.1421	.3102
12	.2200	.1100	.4000	.3000	2.200	.2000	.1330	.4222	.3313	1.100	.2332	.1000	.4410	.3142	4.000	.2111	.1240
13	.3200	.4322	.1413	.2433	3.200	.3404	.4142	.1241	.2124	4.322	.3120	.4424	.1000	.2343	1.413	.3340	.4234
14	.4200	.2100	.3231	.1322	4.200	.4313	.2000	.3111	.1420	2.100	.4403	.2404	.3034	.1000	3.231	.4030	.2323
15	.0300	.0422	.0100	.0211	.3000	.0322	.0402	.0130	.0231	.4222	.0340	.0433	.0114	.0201	.1000	.0310	.0412
16	.1300	.3100	.2413	.4000	1.300	.1231	.3214	.2000	.4432	3.100	.1133	.3313	.2143	.4302	2.413	.1000	.3401
17	.2300	.1422	.4231	.3433	2.300	.2140	.1121	.4414	.3243	1.422	.2411	.1342	.4123	.3013	4.231	.2234	.1000

Using this table, we now illustrate some of the properties of the finite segment p-adic number systems:

- Let $\alpha = 2/3$ and $\beta = 3/4$. The result is $2/3 + 3/4 = 17/12$.

$$\begin{aligned} \frac{2}{3} &= .4131 \\ \frac{3}{4} &= .2111 \\ &= .1342 \end{aligned}$$

  which is found in the table, giving the correct result.

- Let $\alpha = 3/13$ and $\beta = 1/12$. The result is $3/13 + 1/12 = 49/156$.

$$\begin{aligned} \frac{3}{13} &= .1143 \\ \frac{1}{12} &= .3424 \\ &= .4023 \end{aligned}$$

  which is not in the table.

- Let $\alpha = 5/2$ and $\beta = 5/7$. The result is $5/2 + 5/7 = 45/14$.

$$\begin{aligned} \frac{5}{2} &= .0322 \\ \frac{5}{7} &= .0330 \\ &= .0113 \end{aligned}$$

  which is in the table, giving an incorrect result $10/17$. Note that $10/17 = 0.588235$ is far from the correct result $45/14 = 3.21429$ in the *absolute* norm. However, it is 5-adically close, i.e., their difference $10/17 - 45/14 = -625/238$ is divisible by 5^4.

Theorem 2 *Let $\alpha = a/b$ and $\beta = c/d$, with* $\gcd(b,p) = \gcd(d,p) = 1$. *Then $H(p,r,\alpha) = H(p,r,\beta)$ if and only if*

$$a \cdot b^{-1} = c \cdot d^{-1} \pmod{p^r} ,$$

or, in other words,

$$a \cdot d = c \cdot b \pmod{p^r} .$$

Using the previous example $\alpha = 10/17$ and $\beta = 45/14$, we see that

$$10 \cdot 17^{-1} = 45 \cdot 14^{-1} \pmod{625} ,$$

i.e.,

$$10 \cdot 14 = 45 \cdot 17 \pmod{625} .$$

11 Floating-Point Hensel Codes

Let $\alpha = a/b = p^n \cdot \frac{c}{d}$ with $\gcd(c,d) = \gcd(c,p) = \gcd(d,p) = 1$, then the normalized floating-point Hensel code of α is defined as the pair $\hat{H}(p,r,\alpha) = (m,e)$ such that $m = H(p,r,c/d)$ and $e = n$. Here m is the mantissa and e is the exponent. For example,

$$\begin{aligned}
\hat{H}(5,4,2/3) &= (.4131, 0) \\
\hat{H}(5,4,-2/3) &= (.1313, 0) \\
\hat{H}(5,4,2/15) &= (.4131, -1) \\
\hat{H}(5,4,-2/15) &= (.1313, -1) \\
\hat{H}(5,4,10/3) &= (.4131, 1) \\
\hat{H}(5,4,-10/3) &= (.1313, 1) .
\end{aligned}$$

12 Arithmetic using Floating-Point Hensel Codes

Consider the following example: $\frac{2}{3} + \frac{1}{5} = \frac{13}{15}$. The Hensel codes are given as

$$\begin{aligned}
\hat{H}(5,4,2/3) &= (.4131, 0) \\
\hat{H}(5,4,1/5) &= (.1000, -1)
\end{aligned}$$

First, we line up the p-adic points: $(.1000, -1) = (1.000, 0)$ and then perform the addition

$$\begin{array}{r} .4131 \\ 1.000 \\ \hline 1.413 \end{array}$$

Hence, the sum is equal to $(1.413, 0) = (.1413, -1)$ which is equal to $13/15$.

Subtraction is performed by using "complemented addition" in the sense that the subtrahend is complemented and added to the minuend. For example, to compute $\frac{2}{3} - \frac{1}{5} = \frac{7}{15}$ using Hensel codes, we need $\hat{H}(5,4,-1/5) = (.4444, -1)$. We perform the operation

$$\begin{array}{r} .4131 \\ 4.444 \\ \hline 4.313 \end{array}$$

which gives $(4.313, 0) = (.4313, -1)$, i.e., the Hensel code of 7/15.

For multiplication, consider the example: $\frac{1}{3} \cdot \frac{6}{5} = \frac{2}{5}$.

$$\begin{aligned} \hat{H}(5, 4, 1/3) &= (.2313, 0) \\ \hat{H}(5, 4, 6/5) &= (.1100, -1) \end{aligned}$$

The algorithm multiplies the mantissas

$$\begin{array}{r} .2313 \\ .1100 \\ \hline .2313 \\ 231 \\ \hline .2000 \end{array}$$

and adds the exponents: $0 + (-1) = -1$. Thus, $\hat{H}(5, 4, \alpha) = (.2000, -1)$ which is equal to 2/5 since ordinary Hensel code of 2/5 is equal to 2.000.

13 Normalization of Floating-Point Hensel Codes

Consider the following operation $1/2 + 1/8 = 5/8$ using floating-point Hensel codes, $\hat{H}(5, 4, 1/2) = (.3222, 0)$ and $\hat{H}(5, 4, 1/8) = (.2414, 0)$.

$$\begin{array}{r} .3222 \\ .2414 \\ \hline .0241 \end{array}$$

The table indicates that this is indeed the ordinary Hensel code of 5/8. However, we need to compute its floating-point Hensel code of the form $(.xyyy, e)$ where x is nonzero. How can this be achieved? The following method is proposed:

Gregory & Krishnamurty: Convert the unnormalized Hensel code to its order N Farey fraction and then map this number to its normalized floating-point Hensel code. For example, the table indicates that .0241 is equal to 5/8. We then compute (using the table) the Hensel code of 1/8 as .2414 which means the floating-point Hensel code of $5 \cdot \frac{1}{8}$ is equal to $(.2414, 1)$.

Colagrossi & Miola: Soon to be investigated.

14 Research Directions

- Area and time complexity of the binary versus p-adic floating-point number systems.
- Efficient algorithms for conversion, magnitude detection, and normalization of Hensel codes.
- Detection of overflow and underflow.
- Applications of p-adic arithmetic in computational algebra and scientific computing.

More about p-adic arithmetic and Hensel codes can be found in the following books [1, 4, 6] and the papers [8, 5, 3, 10, 11, 7, 12, 13, 9, 2].

References

[1] G. Bachman. *Introduction to p-Adic Numbers and Valuation Theory*. Academic Press, New York, NY, 1964.

[2] R. N. Gorgui-Naguib and R. A. King. Comments on "Matrix processors using p-adic arithmetic for exact linear computations". *IEEE Transactions on Computers*, 35(10):928–930, October 1986.

[3] R. T. Gregory. The use of finite-segment p-adic arithmetic for exact computation. *BIT*, 18(3):282–300, 1978.

[4] R. T. Gregory. *Error-Free Computation*. Huntington, NY: Robert E. Krieger Publishing Company, 1980.

[5] R. T. Gregory. Error-free computation with rational numbers. *BIT*, 21(2):194–202, 1981.

[6] R. T. Gregory and E. V. Krishnamurthy. *Methods and Applications of Error-Free Computation*. Springer, Berlin, Germany, 1984.

[7] E. C. R. Hehner and R. N. S. Horspool. A new representation of the rational numbers for fast easy arithmetic. *SIAM Journal on Computing*, 8(2):124–134, May 1979.

[8] P. Kornerup and R. T. Gregory. Mapping integers and Hensel codes onto Farey fractions. *BIT*, 23(1):9–20, 1983.

[9] E. V. Krishnamurthy. Matrix processors using p-adic arithmetic for exact linear computations. *IEEE Transactions on Computers*, 26(7):633–639, July 1977.

[10] E. V. Krishnamurthy, T. M. Rao, and K. Subramanian. Finite segment p-adic number systems with applications to exact computation. *Proc. Indian Acad. Sci.*, 81A(2):58–79, 1975.

[11] E. V. Krishnamurthy, T. M. Rao, and K. Subramanian. p-Adic arithmetic procedures for exact matrix computations. *Proc. Indian Acad. Sci.*, 82A(5):165–175, 1975.

[12] A. Miola. Algebraic approach to p-adic conversion of rational numbers. *Information Processing Letters*, 18(3):167–171, 30 March 1984.

[13] C. J. Zarowski and H. C. Card. On addition and multiplication with Hensel codes. *IEEE Transactions on Computers*, 39(12):1417–1423, December 1990.