p-adic arithmetic: a tool for error-free computations *

A. Colagrossi, C. Limongelli, A. Miola

1 Introduction

In this paper we propose the use of the p-adic arithmetic as a basic computational tool for a symbolic computation system in the framework of TASSO project. This arithmetic has been chosen for two main reasons.

1. p-adic arithmetic representation provides a unified form to treat numbers and functions by means of truncated power series and it constitutes the mathematical background for the definition of basic abstract data structures for a homogeneous computing environment.

   > The problem of the approximation of numbers and functions brings to the need for an integrate environment allowing a unified representation. We have seen that a unified representation can be obtained when numbers and functions are represented by power series and p-adic analysis offers an appropriate mathematical settlement to handle with power series. In (Limongelli & Temperini, 1995) is shown how it is possible to treat numbers by truncated power series, as like as the most general p-adic construction methods in an integrated computing environment.

2. p-adic arithmetic is an exact arithmetic and the algebraic bases on which it is founded overcome the problem of the floating point arithmetic, which is essentially due to a lack of algebraic setting. Moreover the truncated version of this arithmetic that we treat in this paper is suitable to represent numbers in a finite field. This last characteristic belongs to modular arithmetic too (Knuth, 1981; Gregory & Krishnamurthy, 1984), but the difference is that while modular arithmetic works over the integers, p-adic

*This work has been partially supported by Progetto Finalizzato "Sistemi Informatici e Calcolo Parallelo" of CNR under grant n. 92.01604.69.

arithmetic operates on rational numbers. In (Limongelli, 1995) are shown the advantages due to the possibility of working directly over the rationals. Moreover in (Limongelli & Temperini, 1995; Limongelli, 1993a) is shown that also algebraic numbers are representable in this arithmetic. Moreover in (Limongelli, 1995, 1993b) the possibility of speeding up the computations via its parallelization has been proved from both a theoretical and practical point of view.

Despite to its characteristic of modularity and its powerful algebraic properties (completeness of the p-adic metric space (Koblitz, 1977)), this arithmetic has not received much attentions because of some computational problems, due to the possible lack of the significant digit of the code.

In this paper we show how it is possible to overcome this problem. Actually the only critic point is due to the division operation. We propose a suitable algorithm for division operation and we will show how it is possible to carry out computations with a very low probability of obtaining an actual lack of approximation.

Next section describes the algebraic bases of the proposed arithmetic. Section 3. shows the algebra of Hensel code set and section 4. is devoted to the treatment of the pseudo-Hensel codes which occurs when a significant digit of the code is missed. Last section concludes the paper with a description of the possible further steps in order to extend the applicability of this arithmetic.

2 Basic notions

A rational number $\alpha = a/b$, can always be uniquely expressed as

$$\alpha = \frac{c}{d} \cdot p^e$$

where e is an integer, p is a fixed prime number, and c, d, and p are pairwise relatively prime integers. This kind of representation of rational numbers is called the normalized form. Moreover $\hat{\mathbb{Q}}$ will indicate the set of rational numbers c/d such that $GCD(d,p) = 1$.

The function

$$\|\cdot\|_p : \mathbb{Q} \to \mathbb{R}$$

from the rational numbers $\mathbb{Q}$ to the real numbers $\mathbb{R}$, defined as

$$\|\alpha\|_p = \begin{cases} p^{-e} & \text{if } \alpha \neq 0 \\ 0 & \text{if } \alpha = 0, \end{cases}$$

is a norm on $\mathbb{Q}$ (see (Koblitz, 1977)), called the p-adic norm. On the basis of this p-adic norm, it is possible to define a p-adic metric on $\mathbb{Q}$, such that, given two rational numbers α and β, their distance $d(\alpha, \beta)$ is expressed as:

$$d(\alpha, \beta) = \|\alpha - \beta\|_p.$$

Then $(\mathbb{Q}, d)$ is a metric space, $\mathbb{Q}_p$ is the set of equivalence classes of Cauchy sequences in $(\mathbb{Q}, d)$, the system $(\mathbb{Q}, +, \cdot)$ constitutes a field called the field of p-adic numbers, and $(\mathbb{Q}_p, d)$ is a complete metric space.

The main characteristics of the field of p-adic numbers are the following ones:

- the series
$$\sum_{i=0}^{\infty} p^i$$
converges to $1/(1\text{-}p)$ in $(\mathbb{Q}_p, d)$;

- every rational number α can be uniquely expressed in the form:
$$\alpha = \sum_{i=e}^{\infty} a_i p^i; \quad a_i \in \mathbb{Z}_p; \quad e \in \mathbb{Z}; \quad \|\alpha\|_p = p^{-e}; \quad a_e \neq 0, \qquad (1)$$
where $\mathbb{Z}$ represents the set of integer numbers.

The p-adic representation of a rational number α is an infinite sequence of digits (the p-adic digits) which are the coefficients of the series given in (1):

$$\alpha = (a_e a_{e-1} \ldots a_{-1} \quad . \quad a_0 a_1 a_2 \ldots).$$

Let us recall that the p-adic expansion of a rational number is periodic. Therefore the p-adic representation can also assume the following form:

$$\alpha = (a_e a_{e-1} \ldots a_{-1} \quad . \quad a_0 \ldots a_{k-m-1}{}' a_{k-m} \ldots a_{k-1} a_k)$$

where the m digits on the right hand side of the apex constitutes the period.

Let us now describe the procedure which computes the p-adic representation of a given rational number α:

p-ADIC REPRESENTATION OF A RATIONAL NUMBER

Input: p: prime number;
$\alpha = a/b$, represented in its normalized form, $c/d \cdot p^e$;
Output: the coefficients $a_e, a_{e+1}, a_{e+2}, \ldots$ of the p-adic expansion of α;
Begin

$c_1/d_1 := c/d;$

$i := 0;$

repeat

$a_{e+i} := \mid c_{i+1}/d_{i+1} \mid_p;$

$c_{i+2}/d_{i+2} := \frac{1}{p}\left(c_{i+1}/d_{i+1} - a_{e+i}\right);$

$i := i + 1;$

until the period is detected;

End

Here $\mid c_i/d_i \mid_p = \mid c_i \quad \mid d_i^{-1} \mid_p \mid_p$ is the least non-negative remainder of $c_i/d_i \ mod \ p$.

We note that the hypothesis of primality for p is necessary in order to ensure the existence and the uniqueness of $\mid d_i^{-1} \mid_p$. From now on we will consider p a prime number.

EXAMPLE 1 Let us compute the p-adic expansion of the rational number $3/4$, with $p = 5$ (in this case $e = 0$):

$$\alpha = \frac{3}{4} \cdot 5^0, \quad \frac{c_1}{d_1} = \frac{3}{4};$$

$$a_0 = \mid \frac{c_1}{d_1} \mid_p = \mid \frac{3}{4} \mid_5 = \mid 3 \cdot \mid 4^{-1} \mid_5 \mid_5 = \mid 12 \mid_5 = 2;$$

$$\frac{c_2}{d_2} = \frac{1}{5}\left(\frac{3}{4} - 2\right) = \frac{1}{5}\left(-\frac{5}{4}\right) = -\frac{1}{4};$$

$$a_1 = \mid \frac{c_2}{d_2} \mid_p = \mid -\frac{1}{4} \mid_5 = \mid \mid -1 \mid_5 \cdot \mid 4^{-1} \mid_5 \mid_5 = 1;$$

$$\frac{c_3}{d_3} = \frac{1}{5}\left(-\frac{1}{4} - 1\right) = \frac{1}{5}\left(-\frac{5}{4}\right) = -\frac{1}{4};$$

$$a_2 = \mid \frac{c_3}{d_3} \mid_p = \mid -\frac{1}{4} \mid_5 = 1.$$

In general this process will not terminate, but, since we are assuming that α is a rational number, the p-adic expansion will be periodic and we have to continue the detection of the p-adic coefficients until the period is detected. In this case the p-adic expansion of the number $3/4$ is $.211\ldots = .2\,'1$. □

Arithmetic operations on p-adic numbers are carried out, digit by digit, starting from the left-most digit a_e, as in usual base p arithmetic operations.

The division operation on p-adic numbers is performed in a different way w.r.t. usual integer arithmetic.

Starting from the left-most digit of both the dividend and the divisor, we obtain the left-most digit of the quotient, and so on, in a way similar to the other three basic p-adic arithmetic operations.

In order to make automatic the p-adic arithmetic computations, the usual and obvious problem is related to the length of p-adic digit sequence. A natural solution is reached by introducing a finite length p-adic arithmetic on the so-called Hensel codes as we will show below.

Definition 1 (Hensel Codes) *Given a prime number p, a Hensel code of length r of any rational number $\alpha = (c/d) \cdot p^e$ is a pair*

$$(mant_\alpha, exp_\alpha) = (.\ a_0 a_1 \cdots a_{r-1}, e),$$

where the left-most r digits and the value e of the related p-adic expansion are called the mantissa and the exponent, respectively. Moreover

$$\sum_{i=0}^{r-1} a_i \cdot p^i \in \mathbb{Z}_{p^r}.$$

□

Let $\mathbb{H}_{p,r}$ indicate the set of Hensel codes w.r.t. the prime p and the approximation r and let $H(p, r, \alpha)$ indicate the Hensel code representation of the rational number $\alpha = (a/b) \cdot p^e$ w.r.t. the prime p and the approximation r.

The forward and backward mappings between rational numbers and Hensel codes can then be defined on the basis of the following theorems.

Theorem 1 (Forward Mapping) *Given a prime p, an integer r and a rational number $\alpha = (c/d) \cdot p^n$, such that $GCD(c,p) = GCD(d,p) = 1$, the mantissa $mant_\alpha$ of the code related to the rational number α, is computed by the Extended Euclidean Algorithm (EEA) applied to p^r and d as:*

$$mant_\alpha \equiv c \cdot y \pmod{p^r}$$

where y is the second output of the EEA.

Proof: See (Miola, 1984). □

Let us note that the correspondence between the commutative rings $(\hat{\mathbb{Q}}, +, \cdot)$ and $(\mathbb{H}_{p,r}, +, \cdot)$ does not have an inverse, because each Hensel code mantissa $.\ a_0 a_1 \cdots a_{r-1}$ $(= \sum_{i=0}^{r-1} a_i \cdot p^i \in \mathbb{Z}_{p^r})$ in $\mathbb{H}_{p,r}$, is the image of an infinite subset of the rational numbers.

We need to define a suitable subset of $\hat{\mathbb{Q}}$, such that the correspondence between this subset and $\mathbb{H}_{p,r}$ is injective.

Definition 2 (Farey Fraction Set) *The Farey fraction set $\mathbb{F}_{p,r}$ is the subset of $\hat{\mathbb{Q}}$ such that:*

$$a/b \in \hat{\mathbb{Q}} : GCD(a,b) = 1$$

and

$$0 \le a \le N, \quad 0 < b \le N, \quad N = \left\lfloor \sqrt{\frac{p^r - 1}{2}} \right\rfloor,$$

where $\mathbb{N}$ indicates the set of natural numbers. □

$\mathbb{F}_{p,r}$ will also be called the Farey fraction set of order N, as $N = N(p,r)$.

DEFINITION 3 *The generalized residue class* $\mathbb{Q}_k$ *is the subset* $\hat{\mathbb{Q}}$ *defined as follows:*

$$\mathbb{Q}_k = \{a/b \in \hat{\mathbb{Q}} \text{ such that } \mid a/b\mid_{p^r} = k\}.$$

□

From this last definition it follows that

$$\hat{\mathbb{Q}} = \bigcup_{k=0}^{p^r-1} \mathbb{Q}_k.$$

THEOREM 2 *Let* N *be the largest integer satisfying the inequality*

$$2N^2 + 1 \leq p^r$$

and let $\mathbb{Q}_k$ *contain the order* N *Farey fraction* $x = a/b$. *Then* x *is the only order-*N *Farey fraction in* $\mathbb{Q}_k$.

PROOF: See (Gregory & Krishnamurthy, 1984). □

THEOREM 3 (BACKWARD MAPPING) *Given a prime* p, *an integer* r, *a positive integer* $m \leq p^r$ *and a rational number* $c/d \in \mathbb{F}_{p,r} \subset \hat{\mathbb{Q}}$, *let* m *be the value in* $\mathbb{Z}_{p^r}$ *of the Hensel code mantissa related to* c/d, *then the EEA, applied to* p^r *and* m, *computes a finite sequence of pairs* (x_i, y_i) *such that there exists a subscript* j *for which* $x_j/y_j = c/d$.

PROOF: See (Miola, 1984). □

From these considerations we can finally state the following theorem.

THEOREM 4 *Given a prime* p, *an approximation* r, *given an arithmetic operator* Φ *in* $\mathbb{Q}$ *and the related arithmetic operator* $\Phi' in \mathbb{H}_{p,r}$, *for any* $\alpha_1, \alpha_2 \in \mathbb{Q}$, *if*

$$\alpha_1 \Phi \alpha_2 = \alpha_3, \quad \alpha_3 \in \mathbb{F}_{p,r},$$

then there exists only one $H(p, r, \alpha_3) \in \mathbb{H}_{p,r}$ *such that*

$$H(p, r, \alpha_1)\Phi' H(p, r, \alpha_2) = H(p, r, \alpha_3)$$

On these bases, every computation over $\mathbb{H}_{p,r}$ gives a code which is exactly the image of the rational number given by the corresponding computation over $\hat{\mathbb{Q}}$.

A general schema of computation may consist in mapping on $\mathbb{H}_{p,r}$ the rational numbers given as input to the computation and then of performing the computation over $\mathbb{H}_{p,r}$. However, by THEOREM 3, the inverse mapping can be performed only when the expected result belongs to $\mathbb{F}_{p,r}$.

We note that the choice of order of truncation, as well as the choice of the base p, are made in accordance with an a priori estimation of the magnitude of the solution of the problem. In fact we must identify a suitable set of Farey fractions that contains the rational solution; the choices of p and r are a consequence of this identification.

Such an estimate can be evaluated once a given algorithm is stated for the solution of the problem. This may turn out not to be a simple problem, but such an estimate can be computed on the basis of the number of operations that must be performed in order to reach the rational solution. Let us mention some examples.

- *arithmetic over the rationals:* Let us consider the computation of a^b, where $a \in \mathbb{Q}$ and $b \in \mathbb{Z}$. The number of bits which are necessary to represent the rational result is: $b \cdot log_2 a$.

- *algebra of polynomials:* For example, it is easy to compute in advance the maximum coefficient which can be obtained by a polynomial multiplication. In fact: given the polynomials $\sum_{i=0}^{n} a_i \cdot x^i$ e $\sum_{j=0}^{m} b_j \cdot x^j$, if $a = max\{\mid a_i \mid\}_{1 \leq i \leq n}$, $b = max\{\mid b_j \mid\}_{1 \leq j \leq m}$ and $c = max\{a, b\}$, then the greatest coefficient of the polynomial result is smaller than $max\{n, m\} \cdot c^2$.

- *linear algebra:* For example, it is well known that the determinant $D(A)$ of an n-dimensional square matrix A, is bounded by $n! \cdot a^n$, where $a = max\{\mid a_{i,j} \mid\},\ 1 \leq i, j \leq n$.

There is also a class of mathematical problems which are particularly well-suited for being solved by p-adic arithmetic: these are problems which are affected either by overflow during the computations or by ill-condition.

3 Operations with Hensel codes

In this section we treat Hensel codes arithmetic and we face the problem of pseudo-Hensel codes manipulation, which essentially consists in a loss of significant digits (i.e.: the left-most digits) in an Hensel code. This loss of significative digits does not permit one to execute the division as well as literature has been stated in (Gregory & Krishnamurthy, 1984). In this section we will briefly describe the main arithmetic operations, to show that it is possible to overcome this problem, by presenting a new approach both for division computation and for the treatment of the pseudo-Hensel codes. These results, together with the parallelization of p-adic arithmetic, proposed by the author, extend its use in a wide class of computing problems.

Let us consider now the arithmetic operations in $\mathbb{H}_{p,r}$.

- Addition

Given two Hensel codes

$$H(p,r,\alpha) = (mant_\alpha, exp_\alpha) \text{ and } H(p,r,\beta) = (mant_\beta, exp_\beta),$$

first of all we must operate on them, in order to have $exp_\alpha = exp_\beta$, and then perform the addition taking into account that all the operations are carried out from left to right.

EXAMPLE 2 We want to compute the following addition:

$$\frac{3}{10} + \frac{1}{2}, \text{ in } \mathbb{Z}_{5^4}$$

by choosing $p = 5$ and $r = 4$, we obtain $\mathbb{F}_{5,4} = 17$. The Hensel codes related to 3/10 and to 1/2 are respectively:

$$H(4,5,3/10) \;=\; (.4\ 2\ 2\ 2\ ,\ -1) \text{ and } H(4,5,1/2) \;=\; (.3\ 2\ 2\ 2\ ,\ 0)$$

Since the exponents are different, we must normalize the code which has the greater exponent:

$$(.3\ 2\ 2\ 2\ ,\ 0) \longrightarrow (.0\ 3\ 2\ 2\ ,\ -1)$$

Now we can carry out the addition between the mantissas:

$$\begin{array}{cccccccc} + & . & 4 & 2 & 2 & 2 & , & -1 \\ = & . & 0 & 3 & 2 & 2 & , & -1 \\ \hline & . & 4 & 0 & 0 & 0 & , & -1 \end{array}$$

The code result (.4 0 0 0, -1) represents the rational number 4/5. □

Addition behaves as described in the following operational table in which $\mathbb{SH}_{p,r}$ represents the complement of the set $\mathbb{PH}_{p,r}$ with respect to $\mathbb{H}_{p,r}$ (i.e. $\mathbb{H}_{p,r} = \mathbb{PH}_{p,r} \cup \mathbb{SH}_{p,r}$), being $\mathbb{PH}_{p,r}$ the set of the pseudo-Hensel code, given by the following definition:

DEFINITION 4 (PSEUDO-HENSEL CODES)
A pseudo-Hensel code ($\mathbb{PH}_{p,r}$) *is a code such that* $a_0 = \cdots = a_k = 0$, *with* $0 < k <$ *r-1. The order of a pseudo-Hensel code coincides with* k.

+	$\mathbb{SH}_{p,r}$	$\mathbb{PH}_{p,r}$
$\mathbb{SH}_{p,r}$	$\mathbb{H}_{p,r}$	$\mathbb{SH}_{p,r}$
$\mathbb{PH}_{p,r}$	$\mathbb{SH}_{p,r}$	$\mathbb{PH}_{p,r}$

- Subtraction

In order to perform a subtraction it is sufficient first to compute the complement *mod* p^r of the minuend and then to carry out the addition. If the minuend is a pseudo-Hensel code, then the subtraction can be carried out in the usual way, without using the complement of the minuend (except in the case when the subtrahend is the Hensel code which represents zero).

EXAMPLE 3 We want to compute the following subtraction:

$$\frac{3}{4} - \frac{3}{2}, \text{ in } \mathbb{Z}_{5^4}$$

By choosing $p = 5$ and $r = 4$, we have $\mathbb{F}_{5,4} = 17$. The Hensel codes related to $3/4$ and to $3/2$ are respectively:

$$H(4,5,3/4) \;=\; (.2\ 1\ 1\ 1\ ,\ 0) \;\text{ and }\; H(4,5,3/2) \;=\; (.4\ 2\ 2\ 2\ ,\ 0)$$

In order to carry out the subtraction we must get a p-adic unit from the right digit (instead of from the left digit, as usually happens in subtraction between two integer numbers).

$$\begin{array}{cccccccc} - & . & 2 & 1 & 1 & 1 & , & 0 \\ = & . & 4 & 2 & 2 & 2 & , & 0 \\ \hline & . & 3 & 3 & 3 & 3 & , & 0 \end{array}$$

the code result (.3 3 3 3, 0) represents the rational number $-3/4$. □

The following table shows the operational behaviour of subtraction.

$-$	$\$\mathbb{H}_{p,r}$	$\mathbb{P}\mathbb{H}_{p,r}$
$\$\mathbb{H}_{p,r}$	$\mathbb{H}_{p,r}$	$\$\mathbb{H}_{p,r}$
$\mathbb{P}\mathbb{H}_{p,r}$	$\$\mathbb{H}_{p,r}$	$\mathbb{P}\mathbb{H}_{p,r}$

- Multiplication

In order to perform multiplication we must operate by multiplying the respective mantissas of the codes, and then we must add their exponents. Also in this case the code result is truncated to r digits.

EXAMPLE 4 We want to carry out the following operation:

$$\frac{4}{15} * \frac{5}{2}, \text{ in } \mathbb{Z}_{5^4}$$

By choosing $p = 5$ and $r = 4$, we have $\mathbb{F}_{5,4} = 17$. The Hensel codes related to $4/15$ and to $5/2$ are respectively:

$$H(4,5,4/15) \;=\; (.3\ 3\ 1\ 3\ ,\ -1) \;\text{ and }\; H(4,5,5/2) \;=\; (.3\ 2\ 2\ 2\ ,\ 1).$$

$$
\begin{array}{cccccccc}
* & . & 3 & 3 & 1 & 3 & , & -1 \\
= & . & 3 & 2 & 2 & 2 & , & 1 \\
\hline
 & & 4 & 0 & 0 & 0 & & \\
 & & & 1 & 2 & 3 & & \\
 & & & & 1 & 2 & & \\
 & & & & & 1 & & \\
\hline
= & . & 4 & 1 & 3 & 1 & , & 0
\end{array}
$$

The code result (.4 1 3 1, 0) represents the rational number 2/3. $\square$

The following operational table shows the behaviour of the multiplication and indicates that the multiplication of the elements of $\mathbb{H}_{p,r}$ is always possible.

$*$	$\mathbb{S}\mathbb{H}_{p,r}$	$\mathbb{P}\mathbb{H}_{p,r}$
$\mathbb{S}\mathbb{H}_{p,r}$	$\mathbb{S}\mathbb{H}_{p,r}$	$\mathbb{P}\mathbb{H}_{p,r}$
$\mathbb{P}\mathbb{H}_{p,r}$	$\mathbb{P}\mathbb{H}_{p,r}$	$\mathbb{P}\mathbb{H}_{p,r}$

- Division

In order to perform division we must operate by dividing the respective mantissas of the codes, and then we must subtract the respective exponents.

EXAMPLE 5 We want to carry out the following division:

$$\frac{3}{4}/\frac{6}{5}, \text{ in } \mathbb{Z}_{5^4}$$

By choosing $p = 5$ and $r = 4$, we have $\mathbb{F}_{5,4} = 17$. The Hensel codes related to 3/4 and to 6/5 are respectively:

$$H(4,5,3/4) \;=\; (.2\ 1\ 1\ 1\ ,\ 0) \;\text{ and }\; H(4,5,6/5) \;=\; (.1\ 1\ 0\ 0\ ,\ -1).$$

In order to carry out the division we must compute the inverse *mod* $p(= 5)$ of the least significative digit of the divisor and then we must multiply it by the most left hand digit of the dividend (or of the partial dividend). In this way we will obtain all the digits of the quotient. In this case we must compute $|1^{-1}|_5 = 1$.

$$
\begin{array}{cccc|cccc}
2 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\
\hline
3 & 2 & 4 & 4 & 2 & 4 & 1 & 3 \\
 & 4 & 0 & 0 & & & & \\
 & 1 & 0 & 4 & & & & \\
 & & 1 & 4 & & & & \\
 & & 4 & 3 & & & & \\
 & & & 3 & & & &
\end{array}
$$

The code result (.2 4 1 3, 1) represents the rational number 5/8. □

We must pay particular attention when we operate with elements of $\mathbb{PH}_{p,r}$. In fact if the first digit of the divisor is zero, we cannot compute the modular inverse as stated in the classical algorithm described in (Gregory & Krishnamurthy, 1984).

The following operational table indicates when a division results in a pseudo-Hensel code.

/	$\$\mathbb{H}_{p,r}$	$\mathbb{PH}_{p,r}$
$\$\mathbb{H}_{p,r}$	$\$\mathbb{H}_{p,r}$	$\mathbb{PH}_{p,r}$
$\mathbb{PH}_{p,r}$	$\mathbb{PH}_{p,r}$	$\mathbb{PH}_{p,r}$

4 Manipulation of pseudo-Hensel codes

Looking at the examples presented above, we note that an addition or subtraction, may give a result in which some left-most digits are equal to zero. In this case we will say that the addition (or subtraction) has generated a pseudo-Hensel code (see DEFINITION 4).

We want to define an algorithm which allows us to overcome the problem of pseudo-Hensel code manipulation and also to decrease the frequency with which they occur during computations, in particular at the end of the computation, when the rational result must be detected. In the following we see when a pseudo-Hensel code can occur.

EXAMPLE 6 We want to compute the following addition:

$$\frac{13}{15} + \frac{13}{10}, \quad \text{in} \quad \mathbb{Z}_{5^4}$$

By choosing: $p = 5$, $r = 4$, we obtain $\mathbb{F}_{5,4} = 17$.

The Hensel codes related to 13/15 and to 13/10 are respectively:

$$H(4, 5, 13/15) = (.1\ 4\ 1\ 3\ ,\ -1) \text{ and } H(4, 5, 13/10) = (.4\ 3\ 2\ 2\ ,\ -1)$$

The addition follows:

$$\begin{array}{cccccccc} + & . & 1 & 4 & 1 & 3 & , & -1 \\ = & . & 4 & 3 & 2 & 2 & , & -1 \\ \hline & . & 0 & 3 & 4 & 0 & , & -1 \end{array}$$

In this case one significant digit has been lost. Now, if we apply backward mapping to detect the rational result, we have an error, because the Farey fraction set is decreased: $\mathbb{F}_{5,3} = 7$. In fact the rational result of this computation is 13/10, which does not belong to $\mathbb{F}_{5,3}$. □

Nevertheless we can carry on with the computation, because the code approximation has not been decreased, but if we want to compute a division in which the dividend belongs to $\mathbb{H}_{p,r}$ and the divisor is a pseudo-Hensel code of order k (with $k < r$), as we have previously observed, we can appropriately manipulate these codes, in order to apply the division algorithm. In the following we will show two algorithms proposed in literature for the manipulation of the pseudo-Hensel codes. The first one was proposed by Dittemberger in 1987 and can be summarized by the following steps:

ALGORITHM DIT87

Input: $q_1 \in \mathbb{PH}_{p,r}$:
a pseudo-Hensel code of order k $(1 \leq k \leq r-1)$;
Output: $\overline{q}_1 \in \mathbb{SH}_{p,r-k}$;

1. eliminate the k left-most zeros of the mantissa of q_1;
2. update the exponent of q_1 by adding k to itself; □

We note that if we want to carry on with the computations, all the codes involved in the computation must be modified, that is their approximation must be decreased by a factor of k. In this way we will eliminate the pseudo-Hensel code, but the approximation of all the codes will be decreased.

The algorithm proposed in (Colagrossi & Miola, 1987) tries to rebuild the approximation lost by the pseudo-Hensel code occurrence:

ALGORITHM CM87

Input: $a, b \in \mathbb{SH}_{p,r}$; $q_1 \in \mathbb{PH}_{p,r}$, pseudo-Hensel code
of order k $(1 \leq k \leq r-1)$, such that $q_1 = a + b$;
Output: $\overline{q}_1 \in \mathbb{SH}_{p,r}$;

1. apply the inverse mapping to a and to b, by obtaining the rational numbers related to the codes which has produced the pseudo-Hensel code;
2. apply the direct mapping to these rational numbers, with an approximation equal to $r + k$;
3. carry out the addition: a pseudo-Hensel code of order k is obtained in $\mathbb{PH}_{p,r+k}$;
4. eliminate the first k zeros and update the exponent; now the code will belong to $\mathbb{SH}_{p,r}$; □

The latter algorithm presents some inconveniences. While in the first algorithm the approximation of all the codes involved in the computation decreases and could also become zero (in this latter case it is necessary to begin the computation again by doubling at least the code approximations), in the latter algorithm the computation with the code stops in order to obtain the rational numbers which have generated the pseudo code. But, in this case, we do not know anything about the order of this intermediate result, hence we can not be certain that backward mapping will give the exact result. Furthermore this last algorithm is time consuming.

Moreover let us note that the recovery of the code approximation is necessary only when a division operation with a pseudo code as divisor occurs.

Hence the new proposal consists in proceeding without manipulating the pseudo-Hensel codes, but to manipulate the division algorithm, only when a pseudo-Hensel code occurs as a divisor. In this case the following algorithm is proposed:

Algorithm Lim92

Input: p, r;
$q_1 \in \$\mathbb{H}_{p,r} = (a_0\ a_1\ \ldots a_{r-1},\ 0)$: dividend;
$q_2 \in \mathbb{PH}_{p,r} = (0\ \ldots 0\ b_k \ldots b_{r-1},\ 0)$: divisor (pseudo-Hensel code of order k);
Output: $q_3 = q_1/q_2 \in \mathbb{PH}_{p,r} = (0\ \ldots 0\ c_0 \ldots c_{r-1-k},\ -2k)$;

1. represent the dividend in $\mathbb{H}_{p,r-k}$: $(a_0\ a_1\ \ldots a_{r-k-1},\ 0)$;
2. represent the divisor in $\mathbb{H}_{p,r-k}$: $(b_k\ \ldots b_{r-1},\ k)$;
3. carry out the division (Gregory & Krishnamurthy, 1984) in $\mathbb{H}_{p,r-k}$: $(a_0\ a_1\ \ldots a_{r-k-1},\ 0)/(b_k\ \ldots b_{r-1},\ k)$;
4. represent the code result $(c_0 \ldots c_{r-1-k},\ -2k)$ in $\mathbb{PH}_{p,r}$: $(0\ \ldots 0\ c_0 \ldots c_{r-1-k},\ -2k)$. The result will be a pseudo-Hensel code of order k. □

Example 7 We want to carry out the following computation:

$$\frac{1}{4}/(\frac{1}{2}+\frac{1}{3})+\frac{1}{25}$$

We choose, as usual, $p = 5$ and $r = 4$.

$$H(5,4,1/4) = (.4\ 3\ 3\ 3,\ 0); H(5,4,1/2) = (.3\ 2\ 2\ 2,\ 0);$$

$$H(5,4,1/3) = (.2\ 3\ 1\ 3,\ 0);\ H(5,4,1/25) = (.1\ 0\ 0\ 0,\ -2);$$

$$\frac{1}{2}+\frac{1}{3} = (.3\ 2\ 2\ 2,\ 0) + (.2\ 3\ 1\ 3,\ 0) = (.0\ 1\ 4\ 0,\ 0)$$

$$\frac{1}{4}/(\frac{1}{2}+\frac{1}{3}) = (.4\ 3\ 3\ 3,\ 0)/(.0\ 1\ 4\ 0,\ 0)$$

By applying the above described algorithm we obtain:

Input: $q_1 = (.4\ 3\ 3\ 3,\ 0)$;
$q_2 = (.0\ 1\ 4\ 0,\ 0)$; (pseudo code of order 1);
Output: $q_3 = (.4\ 3\ 3\ 3,\ 0)/(.0\ 1\ 4\ 0,\ 0) = (.0\ 4\ 2\ 2,\ -2)$;

– we represent the dividend in $H(5,3)$, by truncating the right-most digit of the mantissa:

$$(.4\ 3\ 3\ 3,\ 0) \longrightarrow (.4\ 3\ 3,\ 0)$$

– we represent the divisor in $\mathbb{H}_{5,3}$, by truncating the left-most digit of the mantissa. In this case we must update the exponent because the position of the code digits is changed with respect to the power of p:

$$(.0\ 1\ 4\ 0,\ 0) \longrightarrow (.1\ 4\ 0,\ 1)$$

– now we carry out the division (Gregory & Krishnamurthy, 1984) in $\mathbb{H}_{5,3}$:

$$(.4\ 3\ 3,\ 0)/(.1\ 4\ 0,\ 1) = (.4\ 2\ 2,\ -1)$$

– we represent the code result in $\mathbb{PH}_{5,4}$:

$$(.4\ 2\ 2,\ -1) \longrightarrow (.0\ 4\ 2\ 2,\ -2)$$

Furthermore $H(5, 4, 1/25) = (.1\ 0\ 0\ 0,\ -2)$; hence:

$$(.0\ 4\ 2\ 2,\ -2) + (.1\ 0\ 0\ 0,\ -2) = (.1\ 4\ 2\ 2,\ -2)$$

We note that H(5,4,17/50) = (.1 4 2 2, -2). □

Computing in this way we can avoid the loss of significant digits (on the contrary, in the algorithm DIT87 the approximation order of all the codes involved in the computation decreases) and allows the manipulation of the pseudo-Hensel codes in the same way as the Hensel codes. We do not need to recover the rational numbers related to the Hensel codes which have generated the pseudo code (as like as the algorithm CM87 does). Moreover, the approximation lost can be recovered during the rest of the computation, because, with our algorithm, the code length is not decreased.

5 Conclusions

The occurrences of the pseudo-Hensel codes can be sensibly reduced, by taking an appropriate base p and, especially, by parallelizing the arithmetic.

In order to reduce the occurrences of pseudo-Hensel codes choosing an appropriate base p, we can note that the probability of finding a leading zero in a code is equal to $1/(p-1)$. The probability of obtaining a leading zero after an addition between two Hensel code is given by the probability of finding $p-k$ (with $1 \leq k \leq p$) as leading digit of the first code and k as the leading digit of the second code, that is $1/(p-1)^2$. The same occurs for subtraction. From a computational point of view, the best possible choice for p is hence made by taking p to be the greatest prime number less than the maximum integer representable in a memory word.

The parallelization of p-adic arithmetic is not only suitable to reduce the occurrences of the pseudo-Hensel codes, but it speeds up rational number arithmetic especially when big number computations occur. The idea of the parallel p-adic approach (Limongelli, 1993b) is to represent each rational number by a Hensel code for several values of p, each representing one homomorphic image. The computations are then performed independently in each image. The unique result has to be constructed out of the results in the images in a recovery step by using the Chinese Remainder Algorithm. Finally a backward mapping has to be performed that retrieves the rational number from the Hensel code.

References

Colagrossi, A., & Miola, A. (1987). A normalization algorithm for truncated p-adic arithmetic. In *Proc. IEEE 8-th Symposium on Computation Arithmetic* Como. aspetto i proceedings da attilio.

Gregory, R., & Krishnamurthy, E. (1984). *Methods and Applications of Error-Free Computation*. Springer Verlag, New York Inc.

Knuth, D. (1981). *The Art of Computer Programming*, Vol. 2. Addison Wesley Publishing Company, Reading Massacchussets.

Koblitz, N. (1977). *p-adic Numbers, p-adic Analysis and Zeta Functions*. Springer Verlag, New York Inc.

Limongelli, C. (1993a). *The Integration of Symbolic and Numeric Computation by p-adic Construction Methods*. Ph.D. thesis, University of Rome "La Sapienza" Italy. Tecinical Report, Collection of theses, V-93-4.

Limongelli, C. (1993b). On an efficient algorithm for big rational number computations by parallel p-adics. *J. of Symb. Comput.*, *15,2:181-197*.

Limongelli, C. (1995). Exact solution of computational problems via parallel p-adic arithmetic. In Miola, A., & Temperini, M. (Eds.), *Advances in Design of Symbolic Computation Systems*, Vol. This volume of *Texts and Monographs in Symbolic Computation*. Springer Verlag, Wien New York.

Limongelli, C., & Temperini, M. (1995). The uniform representation of mathematical objects by truncated power series. In Miola, A., & Temperini, M. (Eds.), *Advances in Design of Symbolic Computation Systems*, Vol. This volume of *Texts and Monographs in Symbolic Computation*. Springer Verlag, Wien New York.

Miola, A. (1984). Algebraic approach to p-adic conversion of rational numbers. *Information Processing Letters*, *18:167-171*.