Rational base numeration system for p-adic numbers

Karel Klouda[1],[2]
karel.klouda@fit.cvut.cz

Joint work with C. Frougny

[1]FIT & FNSPE, CTU in Prague

[2]LIAFA, Université Paris 7

Mons Theoretical Computer Science Days
September 6-10, 2010, Amiens

Motivation

Task: represent 11 in base 3 over the alphabet $\{0, 1, 2\}$, i.e., in the form of

$$\sum a_i 3^i.$$

Motivation

Greedy algorithm: from left to right

$$3^2 \leq 11 < 3^3 \rightarrow \mathbf{a_2} = \mathbf{1} = \left\lfloor \frac{11}{3^2} \right\rfloor, r_2 = \left\{ \frac{11}{3^2} \right\} = \frac{2}{9}$$

$\mathbf{a_1} = \mathbf{0}, r_1 = 2/3, \mathbf{a_0} = \mathbf{2}, r_0 = 0.$

$$\langle 11 \rangle_3 = 102$$

Motivation

Greedy algorithm: from left to right
Division algorithm: from right to left

$$\begin{aligned}
s_0 = 11 &= 3s_1 + a_0 &\Rightarrow\quad & \mathbf{a_0 = 2}, s_1 = 3\\
s_1 = 3 &= 3s_2 + a_1 &\Rightarrow\quad & \mathbf{a_1 = 0}, s_2 = 1\\
s_2 = 1 &= 3s_3 + a_0 &\Rightarrow\quad & \mathbf{a_2 = 1}, s_3 = 0
\end{aligned}$$

$$\langle 11 \rangle_3 = 102$$

Division algorithm – negative numbers

Algorithm (Division Algorithm)

Given a positive $s \in \mathbb{N}$ and an integer $p > 1$.

1. *Put $s_0 = s$.*
2. *For $i = 0, 1, 2 \ldots$, define s_{i+1} and $a_i \in \mathcal{A}_p = \{0, 1, \ldots, p-1\}$ by*

$$s_i = ps_{i+1} + a_i.$$

Division algorithm – negative numbers

Algorithm (Division Algorithm)

Given a positive $s \in \mathbb{N}$ and an integer $p > 1$.

1. *Put $s_0 = s$.*
2. *For $i = 0, 1, 2\ldots$, define s_{i+1} and $a_i \in \mathcal{A}_p = \{0, 1, \ldots, p-1\}$ by*

$$s_i = ps_{i+1} + a_i.$$

$$s_0 = -1 = 3s_1 + a_0 \quad \Rightarrow \quad \mathbf{a_0} = \mathbf{2}, s_1 = -1$$
$$s_1 = -1 = 3s_2 + a_1 \quad \Rightarrow \quad \mathbf{a_1} = \mathbf{2}, s_2 = -1$$

$$\langle -1 \rangle_3 = \cdots 222 = {}^{\omega}2$$

Division algorithm – negative numbers

Algorithm (Division Algorithm)

Given a positive $s \in \mathbb{N}$ and an integer $p > 1$.

1. *Put $s_0 = s$.*
2. *For $i = 0, 1, 2 \ldots$, define s_{i+1} and $a_i \in \mathcal{A}_p = \{0, 1, \ldots, p-1\}$ by*

$$s_i = ps_{i+1} + a_i.$$

$$s_0 = -1 = 3s_1 + a_0 \quad \Rightarrow \quad \mathbf{a_0 = 2}, s_1 = -1$$
$$s_1 = -1 = 3s_2 + a_1 \quad \Rightarrow \quad \mathbf{a_1 = 2}, s_2 = -1$$

$$\langle -1 \rangle_3 = \cdots 222 = {}^{\omega}2$$

We want:

$$-1 = 2\sum_{i=0}^{\infty} 3^i.$$

Division algorithm – rational input

Algorithm (Division Algorithm)

Given $s \in \mathbb{Z}$ and an integer $p > 1$.

1. *Put $s_0 = n$.*
2. *For $i = 0, 1, 2\ldots$ define s_{i+1} and $a_i \in \mathcal{A}_p = \{0, 1, \ldots, p-1\}$ by*

$$s_i = ps_{i+1} + a_i.$$

Then

$$s = \sum_{i=0}^{\infty} a_i p^i$$

Division algorithm – rational input

Algorithm (Division Algorithm)

Given $\frac{s}{t} \in \mathbb{Q}$ and an integer $p > 1$.

1. *Put $s_0 = n$.*
2. *For $i = 0, 1, 2 \ldots$, define s_{i+1} and $a_i \in \mathcal{A}_p = \{0, 1, \ldots, p-1\}$ by*

$$\frac{s_i}{t} = p\frac{s_{i+1}}{t} + a_i.$$

Then

$$\frac{s}{t} = \sum_{i=0}^{\infty} a_i p^i$$

Division algorithm – rational base

Algorithm (Modified Division (MD) Algorithm)

Given $\frac{s}{t} \in \mathbb{Q}$ *and co-prime integers* $p > q \geq 1$.

1. *Put* $s_0 = n$.
2. *For* $i = 0, 1, 2 \ldots$ *define* s_{i+1} *and* $a_i \in \mathcal{A}_p = \{0, 1, \ldots, p-1\}$ *by*

$$\mathbf{q}\frac{s_i}{t} = p\frac{s_{i+1}}{t} + a_i.$$

Then

$$\frac{s}{t} = \sum_{i=0}^{\infty} \frac{a_i}{q}\left(\frac{p}{q}\right)^i$$

Division algorithm – rational base

Algorithm

Given $\frac{s}{t} \in \mathbb{Q}$ and co-prime integers $p > q \geq 1$.

1. *Put $s_0 = n$.*
2. *For $i = 0, 1, 2 \ldots$ define s_{i+1} and $a_i \in \mathcal{A}_p = \{0, 1, \ldots, p-1\}$ by*

$$\mathbf{q}\frac{s_i}{t} = p\frac{s_{i+1}}{t} + \mathbf{q}a_i.$$

Then

$$\frac{s}{t} = \sum_{i=0}^{\infty} a_i \left(\frac{p}{q}\right)^i$$

What we study

We study representations of r-adic numbers (r prime) in the forms

$$\sum_{i\geq -i_0} a_i \left(\frac{p}{q}\right)^i, \quad \sum_{i\geq -i_0} a_i \left(-\frac{p}{q}\right)^i, \quad \sum_{i\geq -i_0} \frac{a_i}{q} \left(\frac{p}{q}\right)^i, \quad \sum_{i\geq -i_0} \frac{a_i}{q} \left(-\frac{p}{q}\right)^i,$$

with some $i_0 \in \mathbb{N}$ and $a_i \in \mathcal{A}_p = \{0, 1, \ldots, p-1\}$.

p-adic absolute value

Definition

Let p be a prime number.
The p-adic valuation $v_p : \mathbb{Z} \setminus \{0\} \to \mathbb{R}$ is given by

$$n = p^{v_p(n)} n' \quad \textit{with} \quad p \nmid n'.$$

The extension to the set of rational numbers, for $x = \frac{a}{b} \in \mathbb{Q}$

$$v_p(x) = v_p(a) - v_p(b).$$

p-adic absolute value

Definition

Let p be a prime number.
The p-adic valuation $v_p : \mathbb{Z} \setminus \{0\} \to \mathbb{R}$ *is given by*

$$n = p^{v_p(n)} n' \quad \text{with} \quad p \nmid n'.$$

The extension to the set of rational numbers, for $x = \frac{a}{b} \in \mathbb{Q}$

$$v_p(x) = v_p(a) - v_p(b).$$

The p-adic absolute value *on* $\mathbb{Q}$*:*

$$|x|_p = \begin{cases} 0 & \text{if } x = 0, \\ p^{-v_p(x)} & \text{otherwise.} \end{cases}$$

p-adic absolute value – examples

Example

$v_3(6) = 1 \quad \Rightarrow \quad |6|_3 = 3^{-1}, |1/6|_3 = 3^1$

p-adic absolute value – examples

Example

$$v_3(6) = 1 \quad \Rightarrow \quad |6|_3 = 3^{-1}, |1/6|_3 = 3^1$$

$$v_p(p^n) = n \quad \Rightarrow \quad |p^n|_p = p^{-n} \to 0 \text{ as } n \to \infty$$

p-adic absolute value – examples

Example

$$v_3(6) = 1 \quad \Rightarrow \quad |6|_3 = 3^{-1}, |1/6|_3 = 3^1$$

$$v_p(p^n) = n \quad \Rightarrow \quad |p^n|_p = p^{-n} \to 0 \text{ as } n \to \infty$$

$$p = r_1^{j_1} r_2^{j_2} \cdots r_k^{j_k}, q \text{ co-prime to } p \quad \Rightarrow$$

$$\left| \left(\frac{p}{q} \right)^n \right|_r = \begin{cases} r_i^{-j_i n} & \text{if } r = r_i, i \in \{1, 2, \dots, k\}, \\ \geq 1 & \text{otherwise.} \end{cases}$$

$\mathbb{Q}_p$ – the set of p-adic numbers I

The set of p-adic numbers $\mathbb{Q}_p$ is defined as a completion of $\mathbb{Q}$ with respect to $| \ |_p$.

Theorem (Ostrowski)

Every non-trivial absolute value on $\mathbb{Q}$ is equivalent to the classical absolute value $| \ |$ or to one of the absolute values $| \ |_p$, where p is prime.

Standard representation of p-adic numbers I

Theorem

Every $x \in \mathbb{Q}_p$ can be uniquely written as

$$\begin{aligned} x &= a_{-i_0}p^{-i_0} + \cdots + a_0 + a_1 p + a_2 p^2 + \cdots + a_i p^i + \cdots \\ &= \sum_{i \geq -i_0} a_i p^i \end{aligned}$$

with $a_i \in \mathcal{A}_p = \{0, 1, \ldots, p-1\}$ and $i_0 = -v_p(x)$.

Standard representation of p-adic numbers II

Theorem

Let $x \in \mathbb{Q}_p$. Then the standard representation of x is

1. *uniquely given,*
2. *finite if, and only if, $x \in \mathbb{N}$,*
3. *eventually periodic if, and only if, $x \in \mathbb{Q}$.*

MD algorithm

Algorithm (MD algorithm)

Let s be a positive integer. Put $s_0 = s$ and for all $i \in \mathbb{N}$:

$$qs_i = ps_{i+1} + a_i.$$

Return $\frac{1}{q}\frac{p}{q}$-expansion of s: $< s >_{\frac{1}{q}\frac{p}{q}} = \cdots a_2 a_1 a_0$.

$\frac{1}{q}\frac{p}{q}$-expansion – properties

[Akiyama, Frougny, Sakarovitch, 2008]

- for $q = 1$ we get classical representation in base p,

$\frac{1}{q}\frac{p}{q}$-expansion – properties

[Akiyama, Frougny, Sakarovitch, 2008]

- for $q = 1$ we get classical representation in base p,

$$L_{\frac{1}{q}\frac{p}{q}} = \{w \in \mathcal{A}_p^* \mid w \text{ is } \frac{1}{q}\frac{p}{q}\text{-expansion of some } s \in \mathbb{N}\}$$

$\frac{1}{q}\frac{p}{q}$-expansion – properties

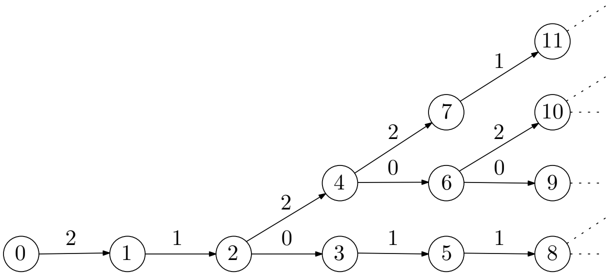
[Akiyama, Frougny, Sakarovitch, 2008]

- for $q = 1$ we get classical representation in base p,

$$L_{\frac{1}{q}\frac{p}{q}} = \{w \in \mathcal{A}_p^* \mid w \text{ is } \frac{1}{q}\frac{p}{q}\text{-expansion of some } s \in \mathbb{N}\}$$

- $L_{\frac{1}{q}\frac{p}{q}}$ is prefix-closed,
- $L_{\frac{1}{q}\frac{p}{q}}$ is not context-free (if $q \neq 1$),

$T_{\frac{1}{q}\frac{p}{q}}$ – tree of nonnegative integers



Children of the vertex n are given by $\frac{1}{q}(pn + a) \in \mathbb{N}, a \in \mathcal{A}_p$.

MD algorithm – the negative case

Let s be a negative integer. The $\frac{1}{q}\frac{p}{q}$-expansion of s is $< s >_{\frac{1}{q}\frac{p}{q}} = \cdots a_2 a_1 a_0$ from the MD algorithm:

$$s_0 = s, \quad qs_i = ps_{i+1} + a_i.$$

MD algorithm – the negative case

Let s be a negative integer. The $\frac{1}{q}\frac{p}{q}$-expansion of s is $< s >_{\frac{1}{q}\frac{p}{q}} = \cdots a_2 a_1 a_0$ from the MD algorithm:

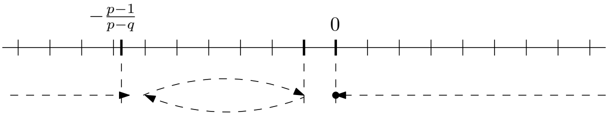
$$s_0 = s, \quad q s_i = p s_{i+1} + a_i.$$

Properties of $(s_i)_{i \geq 0}$:

(i) $(s_i)_{i \geq 1}$ is negative,

(ii) if $s_i < -\frac{p-1}{p-q}$, then $s_i < s_{i+1}$,

(iii) if $-\frac{p-1}{p-q} \leq s_i < 0$, then $-\frac{p-1}{p-q} \leq s_{i+1} < 0$.



In which fields does it work?

$$s = s_k \left(\frac{p}{q}\right)^k + \sum_{i=1}^{k-1} \frac{a_i}{q} \left(\frac{p}{q}\right)^i$$

We want:

$$\left| s - \sum_{i=1}^{k-1} \frac{a_i}{q} \left(\frac{p}{q}\right)^i \right|_r = |s_k|_r \left| \left(\frac{p}{q}\right)^k \right|_r \to 0 \quad \text{as } k \to \infty$$

Hence, if $p = r_1^{j_1} r_2^{j_2} \cdots r_k^{j_k}$, the $\frac{1}{q}\frac{p}{q}$-expansion of s "works" only in $\mathbb{Q}_{r_i}, i = 1, \ldots, k$. The speed of convergence is then $\approx r^{-j_i k}$.

$\frac{1}{q}\frac{p}{q}$-expansions of negative integers

Proposition

Let k be a positive integer, and denote $B = \left\lfloor \frac{p-1}{p-q} \right\rfloor$. Then:

(i) *if $k \leq B$, then $< -k >_{\frac{1}{q}\frac{p}{q}} = {}^{\omega}b$ with $b = k(p-q)$,*

(ii) *otherwise, $< -k >_{\frac{1}{q}\frac{p}{q}} = {}^{\omega}bw$ with $w \in \mathcal{A}_p^+$ and $b = B(p-q)$.*

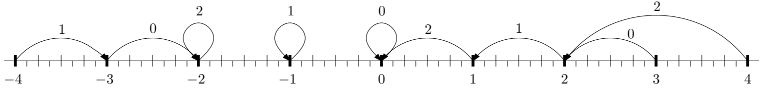
$\frac{1}{q}\frac{p}{q}$-expansions of negative integers

Proposition

Let k be a positive integer, and denote $B = \left\lfloor \frac{p-1}{p-q} \right\rfloor$. Then:

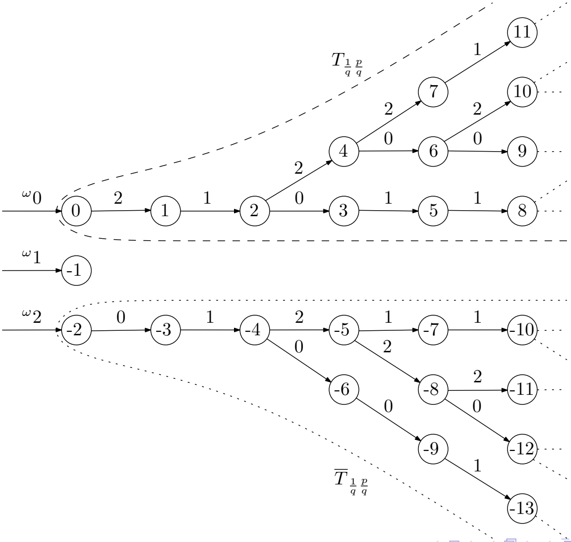
(i) *if $k \leq B$, then $< -k >_{\frac{1}{q}\frac{p}{q}} = {}^{\omega}b$ with $b = k(p-q)$,*

(ii) *otherwise, $< -k >_{\frac{1}{q}\frac{p}{q}} = {}^{\omega}bw$ with $w \in \mathcal{A}_p^+$ and $b = B(p-q)$.*

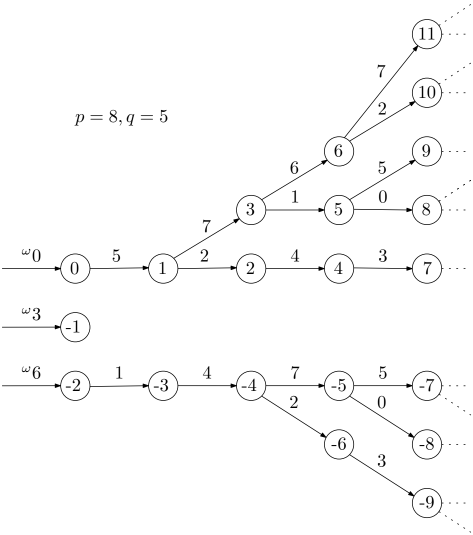


$\overline{T}_{\frac{1}{q}\frac{p}{q}}$ – tree of negative integers

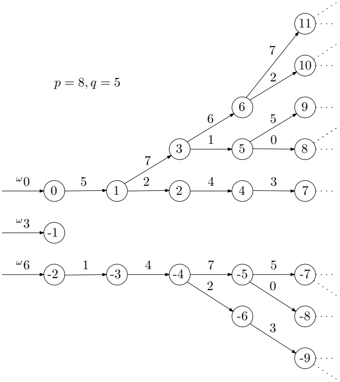
$p = 3, q = 2$



Trees $\overline{T}_{\frac{1}{q}\frac{p}{q}}$ and $T_{\frac{1}{q}\frac{p}{q}}$



Trees $\overline{T}_{\frac{1}{q}\frac{p}{q}}$ and $T_{\frac{1}{q}\frac{p}{q}}$



The trees $\overline{T}_{\frac{1}{q}\frac{p}{q}}$ and $T_{\frac{1}{q}\frac{p}{q}}$ are isomorphic if and only if

$$\frac{p-1}{p-q} \in \mathbb{Z}, \quad \text{i.e., } B(p-q) = p-1$$

MD algorithm for rationals

Algorithm (MD algorithm)

Let $x = \frac{s}{t}$, $s, t \in \mathbb{Z}$ co-prime, $s \neq 0$, and $t > 0$ co-prime to p. Put $s_0 = s$ and for all $i \in \mathbb{N}$ define s_{i+1} and $a_i \in \mathcal{A}_p$ by

$$q\frac{s_i}{t} = p\frac{s_{i+1}}{t} + a_i.$$

Return the $\frac{1}{q}\frac{p}{q}$-expansion of x: $< x >_{\frac{1}{q}\frac{p}{q}} = \cdots a_2 a_1 a_0$.

Examples

x	$< x >_{\frac{1}{q}\frac{p}{q}}$	$(s_i)_{i\geq 0}$	abs. values
		$p = 3, q = 2$	
5	2101	5, 3, 2, 1, 0, 0, ...	all
-5	$^{\omega}$2012	-5,-3,-2,-2,-2, ...	$\lvert\ \rvert_3$
11/4	201	11,6,4,0,0, ...	all
11/8	$^{\omega}$1222	11,2,-4,-8,-8,-8, ...	$\lvert\ \rvert_3$
11/5	$^{\omega}$(02)2112	11,4,1,-1,-4,-6,-4,-6, ...	$\lvert\ \rvert_3$
		$p = 30, q = 11$	
5	11 25	5, 1, 0, 0, ...	all
-5	$^{\omega}$19 8 5	-5,-2,-1,-1,...	$\lvert\ \rvert_2, \lvert\ \rvert_3, \lvert\ \rvert_5$
11/7	$^{\omega}$(12 21 5) 23 13	11, 1, -5, -3, -6, -5, ...	$\lvert\ \rvert_2, \lvert\ \rvert_3, \lvert\ \rvert_5$

MD algorithm – properties

For the sequence $(s_i)_{i\geq 1}$ from the MD algorithm we have:

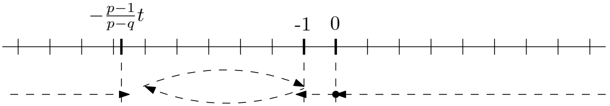
(i) if $s > 0$ and $t = 1$, $(s_i)_{i\geq 1}$ is eventually zero,

(ii) if $s > 0$ and $t > 1$, $(s_i)_{i\geq 1}$ is either eventually zero or eventually negative,

(iii) if $s < 0$, $(s_i)_{i\geq 1}$ is negative,

(iv) if $s_i < -\frac{p-1}{p-q}t$, then $s_i < s_{i+1}$,

(v) if $-\frac{p-1}{p-q}t \leq s_i < 0$, then $-\frac{p-1}{p-q}t \leq s_{i+1} < 0$.



MD algorithm – properties

For the sequence $(s_i)_{i\geq 1}$ from the MD algorithm we have:

(i) if $s > 0$ and $t = 1$, $(s_i)_{i\geq 1}$ is eventually zero,

(ii) if $s > 0$ and $t > 1$, $(s_i)_{i\geq 1}$ is either eventually zero or eventually negative,

(iii) if $s < 0$, $(s_i)_{i\geq 1}$ is negative,

(iv) if $s_i < -\frac{p-1}{p-q}t$, then $s_i < s_{i+1}$,

(v) if $-\frac{p-1}{p-q}t \leq s_i < 0$, then $-\frac{p-1}{p-q}t \leq s_{i+1} < 0$.

Proposition

Let $x \in \mathbb{Q}$. Then $< x >_{\frac{1}{q}\frac{p}{q}}$ is eventually periodic with period $< \frac{p-1}{p-q}t$.

$\frac{1}{q}\frac{p}{q}$-representation I

Definition

A left infinite word $\cdots a_{-\ell_0+1}a_{-\ell_0}, \ell_0 \in \mathbb{N}$, *over* $\mathcal{A}_p$ *is a* *$\frac{1}{q}\frac{p}{q}$-representation* *of* $x \in \mathbb{Q}_r$ *if* $a_{-\ell_0} > 0$ *or* $\ell_0 = 0$ *and*

$$x = \sum_{k=-\ell_0}^{\infty} \frac{a_k}{q}\left(\frac{p}{q}\right)^k$$

with respect to $| \ |_r$.

If the $\frac{1}{q}\frac{p}{q}$-representation is not finite (i.e., does not begin in infinitely many zeros), then the sum converges if and only if r is a prime factor of p.

Number of $\frac{1}{q}\frac{p}{q}$-representations

Let $p = r_1^{j_1} r_2^{j_2} \cdots r_k^{j_k}$.

Theorem

Let $x \in \mathbb{Q}_{r_i}$ for some $i \in \{1, \ldots, k\}$.

(i) *If $k = 1$, there exists a unique $\frac{1}{q}\frac{p}{q}$-representation of x in $\mathbb{Q}_{r_i}$.*

(ii) *If $k > 1$, there exist uncountably many $\frac{1}{q}\frac{p}{q}$-representations of x in $\mathbb{Q}_{r_i}$.*

$\frac{1}{q}\frac{p}{q}$-representations of rational number

Theorem

Let $x \in \mathbb{Q}$ and let $i_1, \ldots, i_\ell \in \{1, \ldots, k\}, \ell < k$, be distinct.

(i) *There exist uncountably many $\frac{1}{q}\frac{p}{q}$-representations which work in all fields $\mathbb{Q}_{r_{i_1}}, \ldots, \mathbb{Q}_{r_{i_\ell}}$.*

(ii) *There exists a unique $\frac{1}{q}\frac{p}{q}$-representation which works in all fields $\mathbb{Q}_{r_1}, \ldots, \mathbb{Q}_{r_k}$; namely, the $\frac{1}{q}\frac{p}{q}$-expansion $< x >_{\frac{p}{q}}$.*

(iii) *The $\frac{1}{q}\frac{p}{q}$-expansion $< x >_{\frac{1}{q}\frac{p}{q}}$ is the only $\frac{1}{q}\frac{p}{q}$-representation which is eventually periodic.*

The other representations

$$\sum_{i\geq -i_0} a_i \left(\frac{p}{q}\right)^i, \quad \sum_{i\geq -i_0} a_i \left(-\frac{p}{q}\right)^i, \quad \sum_{i\geq -i_0} \frac{a_i}{q} \left(\frac{p}{q}\right)^i, \quad \sum_{i\geq -i_0} \frac{a_i}{q} \left(-\frac{p}{q}\right)^i,$$

The other representations

$$\sum_{i\geq -i_0} a_i \left(\frac{p}{q}\right)^i, \quad \sum_{i\geq -i_0} a_i \left(-\frac{p}{q}\right)^i, \quad \sum_{i\geq -i_0} \frac{a_i}{q} \left(\frac{p}{q}\right)^i, \quad \sum_{i\geq -i_0} \frac{a_i}{q} \left(-\frac{p}{q}\right)^i,$$