Unit n° 53

Supplement 6

The simple nested power (snp) representation of $r \in \mathbb{Q}_+, \mathbb{R}_+$

$snp(r,k,n) =$

$a_0 + (a_1 + (a_2 + (a_3 + \ldots + a_{n-1} + (a_n)^{-k})^{-k} \ldots)^{-k})^{-k})^{-k} =$

$[k:a_0;a_1,a_2,a_3,\ldots a_{n-1},a_n]$; $a_i, n \in \mathbb{N}$; $n \to \infty$ infinite snp ; $k \in \mathbb{R}$

is a very efficient tool to analyze the "inner discrete structure" of mathematical constants and functions via

Algorithm 1: transformation $r \in \mathbb{Q}_+, \mathbb{R}_+ \to snp(r,k,n)$

Input $r \in \mathbb{Q}_+, \mathbb{R}_+$; $k \in \mathbb{R}_+$ length((approx.)snp(r,k))	
$x:=r$; $i:=0$	
$a_0:=int(x)$	
repeat	$i:=i+1$
	$x:=(x - int(x))^{-k}$
until	$a_i:=int(x)$
x=int(x) or i=length	
n:=i	
Output (approx.)snp(r,k,n)=$[k:a_0;a_1,a_2,...a_n]$	

Example 1

$r = e = 2.7182818284\ldots$; $k=1, {}^1/_2, 2$

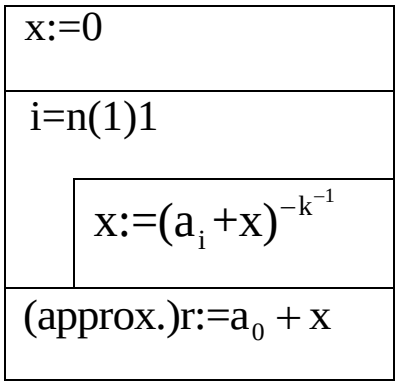
$snp(e,1,\infty) = [1:2; 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, 1,\ldots]$

$snp(e, {}^1/_2, \infty) = [{}^1/_2 : 2; 1, 2, 1, 1, 2, 2, 1, 2, 1, 1, 1, 1, 2, 2, 2, 2, 4, 1, 1, 1, 4, 1, 1, 1, 1, 1, 20, 1, 1, 1, 1, 1, 1, 7, 1, 1, 1, 1, 2, 1, 4, 1, 1, 2, 22, 2, 2, 4, 1, 1, 1, 3, 5, 2, 2, 10, 1, 2, 1, 2, 2, 3, 3, 1, 1, 1, 1, 1, 1, 3, 1, 3, 2, 1,$

1, 2, 1, 1, 1, 1, 1, 1, 1, 2, 1, 1, 1, 2, 1, 1, 3, 1, 3, 1, 1, 1, 2, 1, 1, 1, 1, 3, 1, 1, 2, 1, 2, 2, 1, 2, 1, 5, 4, 17, 1, 2, 8, 1, 2, 7, 3, 2, 1, 2, 1, 1, 5, 1, 6, 6, 1, 4, 1, 3, 1, 12, 2, 2, 3, 1, 5, 1, 1, 2, 1, 1, 1, 3, 1, 1, 1, 1, 1, 1, 1, 1, 2, 3, 1, 13, 1, 2, 1, 1, 1, 1, 1, 2, 3, 14, 1, …]

snp(e,2,∞) = [2: 2; 1, 1, 54, 96, 4, 36, 487, 1, 1, 23, 1, 23, 1, 1, 2, 7, 1, 1, 1, 15, 2, 9, 38, 178, 17, 46, 8, 3, 20, 9, 1, 1, 92, 9, 52, 1, 685, 11, 1, 1, 172, 1, 3, 1, 331, 2, 5, 1, 4, 3, 2, 1, 11, 1, 19, 2, 1, 1, 5, 491, 3, 2, 1, 4, 2, 2, 58, 2, 37, 10, 38, 3, 16, 2, 124, 1, 8, 1, 19, 1, 48, 2, 2, 6, 38, 34, 2, 54, 6, 4, 2, 2, 2, 2377, 48, 102, 1, 4, 1, 1, 529, 4, 5, 1, 4, 7, 5, 4, 63, 1, 16, 1, 27, 2, 2, 1, 121, 394, 1, 3, 509, 32, 921, 1, 21, 1, 21255, 1, 1, 5, 103, 32, 1, 74, 114, 1, 96, 4, 5, 7, 1, 18, 4, 1, 15, 4, 3, 12, 30, 1, 456, 2, 130, 17, 53, 1, 57, 14, 2, 409, 3, 5, 5, 8, 441, 1, 78, 10, 8, 8, 15, 4, 1, 1, 2, 1, 3, 455, 1, 1, 1, 2, 1, 335, 14, 16, 2, 1, 2, 1, 24, 1, 210, 34, 2, 1, 4, 14, 1, …]

Algorithm 2: inverse transformation $[k:a_0;a_1,a_2,a_3,\ldots a_n] \rightarrow$ (approx.)r



Example 2 ⇔

$[k:a_0;a_1,a_2,a_3,\ldots a_{n-1},a_n] = [1/2 :0;6,7,8]$ via Alg. 2 →

r = 0.027590605…

r = 0.027590605… ; k = $1/2$ via Alg. 1 →

$snp(r,k,n) = [k:a_0;a_1,a_2,a_3,\ldots a_{n-1},a_n] = [1/2 :0;6,7,8]$

Example 3 ⇔

$[k:a_0;a_1,a_2,a_3,\ldots a_{n-1},a_n] = [2:0;6,7,8]$ via Alg. 2 →

r = 0.396252795…

r = 0.396252795… ; k = 2 via Alg. 1 →

$snp(r,k,n) = [k:a_0;a_1,a_2,a_3,\ldots a_{n-1},a_n] = [2:0;6,7,8]$

Extension $k \to \underline{k} = (k_1,k_2,k_3,\ldots k_n)$

Algorithm 1: transformation $r \in \mathbb{Q}_+,\mathbb{R}_+ \to snp(r,\underline{k},n)$

Input $r \in \mathbb{Q}_+,\mathbb{R}_+$; $\underline{k} = (k_1,k_2,k_3,\ldots k_n)$ $k_i \in \mathbb{R}_+$ length((approx.)snp(r,$\underline{k}$))
$x:=r$; $i:=0$
$a_0:=int(x)$
repeat $i:=i+1$ $x:=(x - int(x))^{-k_i}$ $a_i:=int(x)$ until
$x=int(x)$ or $i=length$
$n:=i$
Output (approx.)$snp(r,\underline{k},n)=[\underline{k}:a_0;a_1,a_2,\ldots a_n]$

Algorithm 2: inverse transformation $[\underline{k}:a_0;a_1,a_2,a_3,\ldots a_n] \to$ (approx.)r

$x:=0$
$i=n(1)1$ $x:=(a_i + x)^{-k_i^{-1}}$
(approx.)$r:=a_0 + x$
Output (approx.)r

Experiment 1 $\Leftrightarrow$
Transformation

Given

$[\underline{k}:a_0;a_1,a_2,a_3,\ldots a_{n-1},a_n] = [(2,1,2):0;\mathbf{6},\mathbf{7},\mathbf{8}]$

A possible semantics (see **Ch 8**):

$\mathbf{(a_1,a_2,a_3,\ldots a_{n-1},a_n)}$ – zahlenkodierter Klartext

$\underline{k} = (k_1,k_2,k_3,\ldots k_n)$ – kryptographischer Schlüssel

Find via Alg. 2 - Kryptokodierung

r - Cyphertext

Solution

$\mathbf{8}^{-0.5} = 0.35355339\ldots$

$(\mathbf{7}+0.35355339\ldots)^{-1} = 0.135988677\ldots$

$(\mathbf{6}+0.13598867\ldots)^{-0.5} = 0.403699048\ldots$

$0+0.403699048\ldots = \underline{0.403699048\ldots = r}$

Inverse transformation

Given

$r = 0{,}403699048\ldots$; $\underline{k} = (2,1,2)$

Find via Alg. 1 - Dekodierung

$\mathbf{(a_1,a_2,a_3,\ldots a_{n-1},a_n)}$

Solution

$a_0 = \text{int}(0.403699048\ldots) = 0$

$0.403699048\ldots^{-2} = \mathbf{6}.135988676\ldots \rightarrow \mathbf{a_1 = 6}$

$(6.135988676\ldots - 6)^{-1} = \mathbf{7}.353553445\ldots \rightarrow \mathbf{a_2 = 7}$

$(7.353553445\ldots - 7)^{-2} = 7.999997528\ldots \approx \mathbf{8} \rightarrow \mathbf{a_3 = 8}$

$\underline{(a_0;\mathbf{a_1,a_2,a_3}) = (0;\mathbf{6,7,8})}$ q.e.d.

Experiment 2

How about

$\underline{k} = (k_1,k_2{=}a_1,k_3{=}a_2,\ldots)$ etc.?

Check and extend it. It's your turn!

Experiment 3

Find $\underline{k}$ and $\underline{\kappa}$ for

** $[(k_1,k_2,k_3):0;6,7,8]$ via Alg. 2 $\rightarrow$ r

** r, $\underline{\kappa} = (\kappa_1,\kappa_2,\kappa_3,\ldots)$ via Alg. 1 $\rightarrow [(\kappa_1,\kappa_2,\kappa_3,\ldots):0;1,1,\ldots,1)]$

Generalize and extend it. It's your turn!

Experiment 4

Find $\underline{k}$ and $\underline{\kappa}$ for given $[a_0;a_1,a_2,a_3,\ldots]$ and $[b_0;b_1,b_2,b_3,\ldots]$
** $[\underline{k}:a_0;a_1,a_2,a_3,\ldots]$ via Alg. 2 $\rightarrow$ r
** r, $\underline{\kappa} = (\kappa_1,\kappa_2,\kappa_3,\ldots)$ via Alg. 1 $\rightarrow$ $[\underline{\kappa}:b_0;b_1,b_2,b_3,\ldots]$

Experiment 5
Find $\underline{k}$ and $\underline{\kappa}$ for given r and ρ
** r, $\underline{k}$ via Alg. 1 $\rightarrow$ $[\underline{k}:a_0;a_1,a_2,a_3,\ldots]$
** $[\underline{\kappa}:a_0;a_1,a_2,a_3,\ldots]$ via Alg. 2 $\rightarrow \rho$

To be continued.

19.11.2016 EPS(inv.comp), DS(calc)