Unit 60
A collage, first drawing
Controllable recursive decomposition of a number into two summands/factors
60.1

Let us start with the extended Euclidean algorithm

* to find the gcd of two natural numbers a and b without prime factorization using the reduction formula

$$x = y*\mathrm{div}(x,y) + \mathrm{rest}(x,y) = y*\mathrm{int}\left(\frac{x}{y}\right) + x\mathrm{mod}y \; ; \; x,y \in \mathbb{N}$$

step by step from i.g. large numbers (a,b) to small numbers (gcd(a,b),0)

u:=a; v:=b; $\underline{w}:=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$; i := 0

$a_i:=\mathrm{div}(u,v) \rightarrow$

$\underline{w}:=\begin{pmatrix}0 & 1\\ 1 & -\mathrm{div}(u,v)\end{pmatrix}\underline{w}$

$\begin{pmatrix}u\\ v\end{pmatrix}:=\begin{pmatrix}v\\ \mathrm{rest}(u,v)\end{pmatrix}=\begin{pmatrix}0 & 1\\ 1 & -\mathrm{div}(u,v)\end{pmatrix}\begin{pmatrix}u\\ v\end{pmatrix}$

i:=i+1

v=0

$\gcd(a,b):=u$

n:=i-1

$\mathrm{scf}\left(\frac{a}{b}\right)=[a_0;\ a_1,\ a_2,\ldots,\ a_n]$

$\underline{m}:=\underline{w}$

$\begin{pmatrix}\gcd(a,b)\\ 0\end{pmatrix}=\begin{pmatrix}m_{11} & m_{12}\\ m_{21} & m_{22}\end{pmatrix}\begin{pmatrix}a\\ b\end{pmatrix}=\underline{m}\begin{pmatrix}a\\ b\end{pmatrix}$; $\mathrm{abs}(\det\underline{m})=1$

$\frac{a}{\gcd(a,b)}:=\mathrm{abs}(m_{22})$; $\frac{b}{\gcd(a,b)}:=\mathrm{abs}(m_{21})$

$\begin{pmatrix}x\\ y\end{pmatrix}=\underline{m}^{T}\begin{pmatrix}c\\ t\end{pmatrix}$ is solution of the linear Diophantine equation $ax+by=c*\gcd(a,b)$; $a,b\in\mathbb{N}$; $x,y,c,t\in\mathbb{Z}$

* to calculate simultaneously the expansion of the common fraction a/b into a simple continued fraction scf (a/b) and
* the 2by2 Euclidean transformation matrix $\underline{m}$,

$$\begin{pmatrix} \gcd(a,b) \\ 0 \end{pmatrix} = \underline{m} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix},$$

at the same time solution matrix of the linear Diophantine equation a*x + b*y = c*gcd(a,b)

$$\begin{pmatrix} x \\ y \end{pmatrix} = \underline{m}^{T} \begin{pmatrix} c \\ t \end{pmatrix} ; \; a,b \in \mathbb{N} \; ; \; c,x,y,t \in \mathbb{Z} \; .$$

Example 1

a = 1272, b = 684

gcd(a,b) = 12

n = 3, scf(a/b) = [1;1,6,8]

$$\underline{m} = \begin{pmatrix} 7 & -1 \\ -57 & 106 \end{pmatrix} 3 = \begin{pmatrix} 0 & 1 \\ 1 & -8 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -6 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

The 2by2 matrix and the 2by2 matrix chain product enter the stage, here together with the scf expansion.

$$\begin{pmatrix} 12 \\ 0 \end{pmatrix} = \begin{pmatrix} 7 & -13 \\ -57 & 106 \end{pmatrix} \begin{pmatrix} 1272 \\ 684 \end{pmatrix}$$

$$\frac{a}{\gcd(a,b)} = 106 \; ; \quad \frac{b}{\gcd(a,b)} = 57$$

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 7 & -57 \\ -13 & 106 \end{pmatrix} \begin{pmatrix} c \\ t \end{pmatrix} \; ; \; x = 7c - 57t \; ; \; y = -13c + 106t$$

is solution of the linear Diophantine equation
$1272x+684y=12c$; $x,y,c,t \in \mathbb{Z}$

e.g. decomposes the integer 12c into the two integer weighted summands 1272x and 684y controlled by the integer t.

For c=2 we have

t	x	y
-3	185	-344
-2	128	-238
-1	71	-132
0	14	-26
1	-43	80
2	-100	186
3	-157	292

60.2
A fast input follower

Input: b; x[0]; ε
x : = x[0]
y : = x
$\begin{pmatrix} u \\ v \end{pmatrix} := \begin{pmatrix} n-1 & n+1 \\ n+1 & n-1 \end{pmatrix} \begin{pmatrix} y^n \\ b^n \end{pmatrix}$
$x := y * \frac{u}{v}$
$\lvert x - y \rvert \leq \varepsilon$
? (b, ε) : = x
Output : (b,ε)

Experiment:

n = 2; b = 5; x[0] = 50

i	x[i]
0	50.0
1	17.10963455
2	6.966075316

3	5.044552888
4	5.000000871
5	5.000000001
6	5.0

After a short transient process (shape and duration depend on b, x[0], and ε) we obtain $(b,\varepsilon) = b$, i.e. output = input → dynamic input follower, strong attractor, cubic convergence.

Controllable decomposition of a positive real number b into two summands/factors

An application field of the dynamic input follower in the configuration carrier-rocket − shuttle is the decomposition (splitting) of the input b regarding a given expression containing k variables (simplest case: expression = v1 +v2) into k values of this variables (simplest case: va1 and va2) so that the value of the given expression is b for this k values of the variables (simplest case: va1 +va2 = b)

Experimental test:
b = 60,
expression = $v_1 + v_2$,
dynamic input follower recursion formula:

$$x[i+1]=x[i-1]\frac{1+3\left(\frac{b}{x[i-1]+x[i]}\right)^2}{3+\left(\frac{b}{x[i-1]+x[i]}\right)^2};\ i=1,2,3,...$$

with the initial values

x[0] = x[1] =70

Record of the sequences $<x[i]>_{i=0}$

i	x[i]	x[i-1] + x[i]	b-comment
0	70.0		60.0
1	70.0	140.0	60.0
2	34.1025641	104.1025641	After a transient
3	41.94208978	76.04465388	process, b = 60 is
4	26.9956893	68.93777908	decomposed into
5	36.52862605	63.52431535	two summands,
6	25.4991587	62.02778475	25.04.. and
7	35.33477274	60.83393144	34.96..,
8	25.14962442	60.48439716	their sum is 60.
9	35.05179417	60.20141859	

10	25.06548043	60.1172746	Decomposition
11	34.98341646	60.04889689	depends on b, x[0], and x[1]; can be changed by ← injection into x[i]
	→ +4 =		
	38.987341646	64.04889689	
12	23.48258115	62.46992279	
13	37.44648258	60.92906373	
14	23.12453303	60.57101561	
15	37.09347465	60.21800768	
16	23.04081539	60.13429004	
17	37.01063875	60.05145414	60.0
18	23.02107323	60.03171198	60.0
19	36.99108774	60.01216097	65.0 ← change of b
20	24.93127496	61.9223627	65.0
21	38.82849488	63.75976984	New transient process
22	25.41618296	64.24467784	65.0
23	39.28498429	64.70116725	65.0
24	25.53357107	64.81855536	Decomposition

25	39.39495335	64.92852442	of b into two summands 25.56.. and 39.42..
26	25.56167931	64.95663266	
27	39.42125481	64.98293412	
28	25.56839234	64.98964715	
29	39.42753462	64.99592696	
30	25.56999461	64.99752923	
31	39.42903339	64.999028	65.0
		x[i-1]*x[i]	← Change of operation
		1008.200171	65.0
32	8.617674603	339.7865797	Fast factorization of b, cubic convergence! Strong attractor, self-focusing
33	14.41011539	124.1816854	
34	4.795627886	69.10555121	
35	13.55479026	65.00373017	
36	4.795352694	64.99999999	
37	13.55479026	64.99999999	
38	4.795352694	64.99999999	

How about integer factorization of $b \in \mathbb{N}$, esp. semiprime (= product of two primes)? → security guarantee of the RSA public key based cryptosystems.

60.3
A semiprime factoring alternating Gradient synchrotron ?

Download

German version [.pdf].

English version [.pdf].

17.11.2005

stoschek@tcs.inf.tu-dresden.de

60.4

Design a partition algorithm for the following problem.

Given a natural number n.

Find two natural numbers k and m with

** k*m = n

** $k \geqslant m$

** the smallest possible difference k – m

Example

n = 1234567890 , k = 36070 , m = 34227

Special cases

** k = m → square root extraction k = m = sqr(n)

** $n = a^2 - b^2$; $a \gg b$ → k = a + b ; m = a – b

** n is semiprim, e.g. k and m are prime → RSA code breaking (semiprime factorization)

** n is prime, e.g. k = n , m = 1 → primality test

** ?