Unit 53, Supplement 1
Extended Euclidean compact and beyond
A basic graph model of creativity
Creativity means
** to make a potentially existing vertex of the ”knowledge graph”
“visible”, real existing
** using extrapolation, extension, evolution
** by a breakthrough in research or development to new results, theories, methods, …
** by chance, serendipity, intuition, …
** to connect
** adjacent, neighboring
** far distant (far-fetched)
already existing vertices of the knowledge graph by not yet thought, not yet existing edges.

Input: $a, b \in \mathbb{N}$
$u := a\,;\ v := b\,;\ i := 0\,;\ \underline{w} := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
$a_i := \text{int}\left(\frac{u}{v}\right)$
$\underline{w} := \begin{pmatrix} 0 & 1 \\ 1 & -a_i \end{pmatrix} \underline{w}$
$(u, v) := (v\ ,\ u \bmod v)$
$i := i + 1$
$v = 0$
$n := i - 1$
$\gcd(a, b) := u$
$\underline{m} := \underline{w}$

Output

- $\gcd(a,b)$
- $\mathrm{cf}\left(\frac{a}{b}\right) = [a_0; a_1, a_2, a_3, ..., a_n] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ddots + \cfrac{1}{a_n}}}}$
- $\underline{m} = \begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix}\ ;\ \det\underline{m} = \pm 1$
  - $m_{11} = \left(\frac{a}{\gcd(a,b)}\right)^{-1} \bmod \left(\frac{b}{\gcd(a,b)}\right)$ minimal residue![1]

    $m_{12} = \left(\frac{b}{\gcd(a,b)}\right)^{-1} \bmod \left(\frac{a}{\gcd(a,b)}\right)$ minimal residue!

    $\frac{-m_{21}}{\det\underline{m}} = \frac{b}{\gcd(a,b)}$

    $\frac{m_{22}}{\det\underline{m}} = \frac{a}{\gcd(a,b)}$
  - $\begin{pmatrix} x \\ y \end{pmatrix} = \underline{m}^T \begin{pmatrix} \frac{c}{\gcd(a,b)} \\ t \end{pmatrix}\ ;\ t \in \mathbb{Z}$

    is solution of the linear Diophantine equation

    $a\,x + b\,y = c\,;\ a,b \in \mathbb{N}\,;\ c \in \mathbb{Z}\,;\ \gcd(a,b)|c\,;\ x,y \in \mathbb{Z}$

[1] The value B or $B - M$ (whichever is smaller in absolute value), where $A \equiv B \mod M$ is called the minimal residue of $A \mod M$.

Example 1

$a = 1272; b = 684$

- $\gcd(a, b) = 12$
- $\mathrm{cf}\left(\frac{a}{b}\right) = [1; 1, 6, 8] = 1 + \cfrac{1}{1 + \cfrac{1}{6 + \cfrac{1}{8}}}$
- $\underline{m} = \begin{pmatrix} 7 & -13 \\ -57 & 106 \end{pmatrix}$
  - $\frac{a}{\gcd(\mathrm{a,b})} = 106$
  - $\frac{b}{\gcd(\mathrm{a,b})} = 57$

    $\left(\frac{a}{\gcd(\mathrm{a,b})}\right)^{-1} \mod \left(\frac{b}{\gcd(\mathrm{a,b})}\right) = 7$

    $\left(\frac{b}{\gcd(\mathrm{a,b})}\right)^{-1} \mod \left(\frac{a}{\gcd(\mathrm{a,b})}\right) = -13$
  - $\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 7 & -57 \\ -13 & 106 \end{pmatrix} \begin{pmatrix} \frac{c}{12} \\ t \end{pmatrix}; t \in \mathbb{Z}$

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

Example 2

$a = 9060; b = 4872$

- $\gcd(a, b) = 12$
- $\mathrm{cf}\left(\frac{a}{b}\right) = [1; 1, 6, 8, 7] = 1 + \cfrac{1}{1 + \cfrac{1}{6 + \cfrac{1}{8 + \frac{1}{7}}}}$
- $\underline{m} = \begin{pmatrix} -57 & 106 \\ 406 & -755 \end{pmatrix}$
  - $\frac{a}{\gcd(a,b)} = 755$
  - $\frac{b}{\gcd(a,b)} = 406$

    $\left(\frac{a}{\gcd(a,b)}\right)^{-1} \mod \left(\frac{b}{\gcd(a,b)}\right) = -57$

    $\left(\frac{b}{\gcd(a,b)}\right)^{-1} \mod \left(\frac{a}{\gcd(a,b)}\right) = 106$
  - $\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} -57 & 406 \\ 106 & -755 \end{pmatrix} \begin{pmatrix} \frac{c}{12} \\ t \end{pmatrix}; t \in \mathbb{Z}$

    is solution of the linear Diophantine equation
    $9060x + 4872y = c; c \in \mathbb{Z}; 12|c$

Supplement

$x = a^{-1} \mathrm{mod} b = \begin{cases} m_{11} \\ b + m_{11} \end{cases}$ for $\begin{cases} m_{11} > 0 \\ m_{11} < 0 \end{cases}$; $0 < x < b$

is solution of the linear Diophantine equation

$ax \equiv 1 \bmod b$; $a,b,x \in \mathbb{N}$; $\gcd(a,b) = 1$.

Example

$a = 755, b = 406 \rightarrow m_{11} = -57 \rightarrow x = 349$

Test $755 * 349 \bmod 406 = 1$

Exercise 1

Discuss the meaning of the matrices

$\underline{m}^2$ and $\underline{m}\,\underline{m}^T$.

Exercise 2

The loop body of Euclidean compact can be rearranged:

$$\begin{pmatrix} u \\ v \end{pmatrix} := \begin{pmatrix} 0 & 1 \\ 1 & -\mathrm{int}\left(\frac{u}{v}\right) \end{pmatrix} \begin{pmatrix} u \\ v \end{pmatrix} = \begin{pmatrix} \mathrm{int}\left(\frac{u}{v}\right) & 1 \\ 1 & 0 \end{pmatrix}^{-1} \begin{pmatrix} u \\ v \end{pmatrix} \quad \rightarrow$$

$$\begin{pmatrix} u \\ v \end{pmatrix} := \begin{pmatrix} \mathrm{int}\left(\frac{u}{v}\right) & \mathrm{int}\left(\frac{u}{u}\right) \\ \mathrm{int}\left(\frac{v}{v}\right) & \mathrm{int}\left(\frac{v}{u}\right) \end{pmatrix}^{-1} \begin{pmatrix} u \\ v \end{pmatrix}$$

Discuss the following Euclidean compact extension regarding this:

$$\begin{pmatrix} u \\ v \\ \cdots \\ w \end{pmatrix} := \begin{pmatrix} a \\ b \\ \cdots \\ c \end{pmatrix}$$

$$\begin{pmatrix} u \\ v \\ \cdots \\ w \end{pmatrix} := \left(\begin{array}{ccc} \mathrm{int}\left(\frac{u}{w}\right) & \mathrm{int}\left(\frac{u}{v}\right) & \mathrm{int}\left(\frac{u}{u}\right) \\ \mathrm{int}\left(\frac{v}{w}\right) & \mathrm{int}\left(\frac{v}{v}\right) & \mathrm{int}\left(\frac{v}{u}\right) \\ \cdots & \cdots & \cdots \\ \mathrm{int}\left(\frac{w}{w}\right) & \mathrm{int}\left(\frac{w}{v}\right) & \mathrm{int}\left(\frac{w}{u}\right) \end{array}\right)^{-1} \begin{pmatrix} u \\ v \\ \cdots \\ w \end{pmatrix}$$

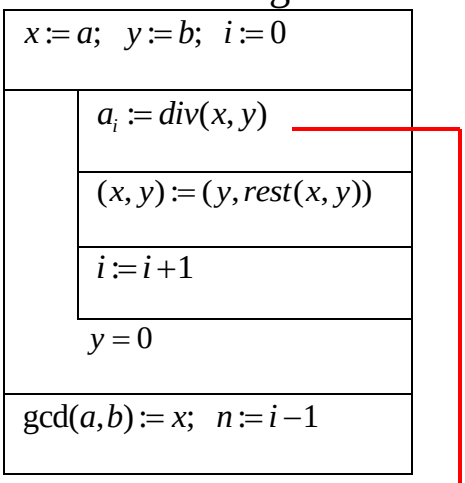
loop condition ?

$$\text{result ?} := \begin{pmatrix} u \\ v \\ \cdots \\ w \end{pmatrix}$$

Discuss other Euclidean compact extensions.

Comparision

** Euclidean algorithm & simple continued fraction



$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_n}}}$$

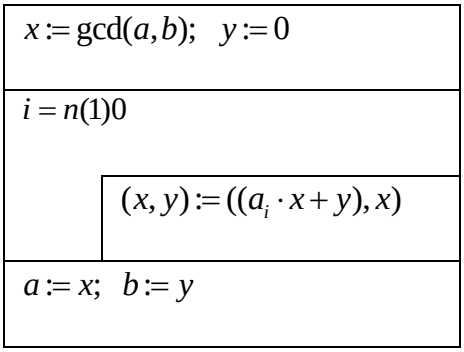
$$= [a_0; a_1, a_2, .., a_n] = scf\left(\frac{a}{b}\right)$$

i	x	y	a_i
0	1272	684	1
1	684	588	1
2	588	96	6
3	96	12	8
4	12	0	

$$\rightarrow \frac{1272}{684} = 1 + \cfrac{1}{1 + \cfrac{1}{6 + \frac{1}{8}}}$$

Inversion

$\gcd(a, b);\quad [a_0; a_1, a_2, .., a_n] \rightarrow a, b$



i	a_i	x	y
3	8	12	0
2	6	96	12
1	1	588	96
0	1	684	588
		1272	684

** Representation of a natural number a in a position system with the basis $b \in \mathbb{N}$

$x := a;\quad y := b;\quad i := 0$
$a_i := rest(x, y)$
$(x, y) := (div(x, y), y)$
$i := i + 1$
$x := 0$
$(b := y);\quad n := i - 1$

$$a_0 + a_1 b^1 + a_2 b^2 + .. + a_n b^n = (a_n .. a_2 a_1 a_0)_b$$

$$= \sum_{i=0}^{n} a_i b^i = a$$

i	x	ai
0	613	1
1	68	5
2	7	7
3	0	0

$\rightarrow$

$$613 = 1 \cdot 9^0 + 5 \cdot 9^1 + 7 \cdot 9^2$$
$$= (751)_9$$

Inversion

$b;\quad (a_n .. a_2 a_1 a_0)_b \rightarrow a, b$

$x := 0;\quad y := b$
$i = n(1)0$
$(x, y) := ((a_i + x \cdot y), y)$

$a := x;\quad b := y$

i	a_i	x	y
2	7	0	9
1	5	7	9
0	1	68	9
		613	

Discussion!

Representation of a natural number a in a position system with the basis $b \in \mathbb{N}$ antithesis

$x := a;\quad y := b;\quad i := 0$
$a_i := rest(x, y)$
$(x, y) := (div(x, y), y)$
$i := i + 1$
$x := 0$
$(b := y);\quad n := i - 1$

$$a_0 + a_1 b^1 + a_2 b^2 + .. + a_n b^n = (a_n .. a_2 a_1 a_0)_b$$

$$= \sum_{i=0}^{n} a_i b^i = a$$

$\rightarrow$

$$613 = 1 \cdot 9^0 + 5 \cdot 9^1 + 7 \cdot 9^2$$

$$= (751)_9$$

i	x	a_i
0	613	1
1	68	5
2	7	7
3	0	0