Unit 53 Euclidean compact and beyond

Euclidean compact

Input: $a,\, b \in \mathbb{N}$

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

$v = 0$

$a_i := \text{int}\left(\frac{u}{v}\right)$

$\underline{w} := \begin{pmatrix} 0 & 1 \\ 1 & -a_i \end{pmatrix} \underline{w}$

$(u, v) := (v\ ,\ u \bmod v)$

$i := i + 1$

$n := i - 1$

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

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

Output

- $\gcd(a, b)$
- $\text{cf}\left(\frac{a}{b}\right) = [a_0; a_1, a_2, a_3, ..., a_n] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ddots + \cfrac{1}{a_n}}}}$
- $\underline{m} = \begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix}\ ;\ \det\underline{m} = \pm 1$
  - $m_{11} = \left(\frac{a}{\gcd(a,b)}\right)^{-1} \bmod \left(\frac{b}{\gcd(a,b)}\right)$ 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 $A \equiv B \bmod M$, is called the

Example 1

$a = 1272\,;\ b = 684$

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

    $\dfrac{b}{\gcd(a, b)} = 57$

    $\left(\dfrac{a}{\gcd(a, b)}\right)^{-1} \bmod \left(\dfrac{b}{\gcd(a, b)}\right) = 7$

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

    is solution of the linear Diophantine equation

    $1272\,x + 684\,y = c\,;\ c \in \mathbb{Z}\,;\ 12|c$

Example 2

$a = 9060\,;\ b = 4872$

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

    $\dfrac{b}{\gcd(a, b)} = 406$

---

minimal residue of $A \bmod M$ [1].

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

$$\left(\frac{b}{\gcd(a,b)}\right)^{-1} \bmod \left(\frac{a}{\gcd(a,b)}\right) = 106$$

- $\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} -57 & 406 \\ 106 & -755 \end{pmatrix} \begin{pmatrix} \frac{c}{12} \\ t \end{pmatrix};\ t \in \mathbb{Z}$

  is solution of the linear Diophantine equation

  $9060\,x + 4872\,y = c;\ c \in \mathbb{Z};\ 12|c$

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:

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

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

Discuss the following Euclidean compact extension regarding this:

$\begin{pmatrix} u \\ v \\ \cdots \\ w \end{pmatrix} := \begin{pmatrix} a \\ b \\ \cdots \\ c \end{pmatrix}$
$\begin{pmatrix} u \\ v \\ \cdots \\ w \end{pmatrix} := \left(\begin{array}{ccc} \text{int}\left(\frac{u}{w}\right) & \text{int}\left(\frac{u}{v}\right) & \text{int}\left(\frac{u}{u}\right) \\ \text{int}\left(\frac{v}{w}\right) & \text{int}\left(\frac{v}{v}\right) & \text{int}\left(\frac{v}{u}\right) \\ \cdots & \cdots & \cdots \\ \text{int}\left(\frac{w}{w}\right) & \text{int}\left(\frac{w}{v}\right) & \text{int}\left(\frac{w}{u}\right) \end{array}\right)^{-1} \begin{pmatrix} u \\ v \\ \cdots \\ w \end{pmatrix}$
loop condition ?
result ? := $\begin{pmatrix} u \\ v \\ \cdots \\ w \end{pmatrix}$

Discuss other Euclidean compact extensions.

Exercise 3

The Fibonacci sequence $< f(i) >_{i=1}^{\infty}$, defined by the recurrence relation
$f(1) = f(2) = 1$
$f(i) = f(i-1) + f(i-2);\ i = 3(1)...$

obey the gcd law
$\gcd(f(i), f(j)) = f(\gcd(i, j))\,.$

Find similar gcd laws for other sequences.

Solutions:

- $\gcd(2^i - 1, 2^j - 1) = 2^{\gcd(i,j)}\,;\ i, j \in \mathbb{N}$
- $\gcd(p^i - q^i, p^j - q^j) = p^{\gcd(i,j)} - q^{\gcd(i,j)}\,;\ p, q \in \mathbb{P}\,;\ p > q\,;\ i, j \in \mathbb{N}$
- $\gcd(a^i - b^i, a^j - b^j) = a^{\gcd(i,j)} - b^{\gcd(i,j)}\,;\ a, b \in \mathbb{N};\ \gcd(a, b) = 1\,;\ i, j \in \mathbb{N}$

Exercise 4

$a = \prod_{i=1}^{\infty} p_i^{\alpha_i}\,;\ p_1 = 2\,,\ p_2 = 3\,,\ p_3 = 5\,,\ p_4 = 7\,,\ \ldots$ – prime sequence; $\alpha_i \in \mathbb{N}_0$

Find an Euclidean–like algorithm for computing

$\mathrm{red}(a) = \prod_{i=1}^{\infty} p_i^{\mathrm{sgn}(\alpha_i)\cdot(\alpha_i - 1)}$

without prime factorization of a.

Example:

$a = 1272\,,\ \mathrm{red}(a) = 4$

Extension and exhaustion 1

$\gcd(a, b)$ – greatest common divisor of $a \in \mathbb{N}$ and $b \in \mathbb{N}$

$\mathrm{lcm}(a, b)$ – least common multiple of $a \in \mathbb{N}$ and $b \in \mathbb{N}$

Let

$a = \prod_{i=1}^{\infty} p_i^{\alpha_i}\,;\ p_1 = 2\,,\ p_2 = 3\,,\ p_3 = 5\,,\ \ldots$ prime sequence; $\alpha_i \in \mathbb{N}_0$

$b = \prod_{i=1}^{\infty} p_i^{\beta_i}$ $\qquad\qquad \beta_i \in \mathbb{N}_0$

the prime factorizations of a and b, then the $\gcd(a, b)$ and $\mathrm{lcm}(a, b)$ are defined by

$\gcd(a, b) = \prod_{i=1}^{\infty} p_i^{\min(\alpha_i, \beta_i)}$

$\mathrm{lcm}(a, b) \prod_{i=1}^{\infty} p_i^{\max(\alpha_i, \beta_i)}$

and

$\gcd(a, b) \cdot \mathrm{lcm}(a, b) = a \cdot b = \prod_{i=1}^{\infty} p_i^{\alpha_i + \beta_i}\,.$

The number–theoretic functions $\gcd(a, b)$ and $\mathrm{lcm}(a, b)$ can be interpreted as binary operations on $\mathbb{N}$:

$\gcd(a, b) = a \perp b$

$\mathrm{lcm}(a, b) = a \top b\,.$

This both and a third binary operation, derived from $\perp$ and $\top$

$$a \circ b = \frac{a \top b}{a \bot b} = \frac{a \cdot b}{(a \bot b)^2} = \prod_{i=1}^{\infty} p_i^{|\alpha_i - \beta_i|} = -m_{21}\, m_{22}\,,$$

$a \,\square\, b\,;\ \square \in \{\bot, \top, \circ\}$

satisfy the following properties:

- If $a \in \mathbb{N}$ and $b \in \mathbb{N}$, then $a \square b \in \mathbb{N}$
  property of closure
- $(\forall a)(\forall b)\, a \,\square\, b = b \,\square\, a\,;\ a, b \in \mathbb{N}$
  commutativity
- $(\forall a)(\forall b)(\forall c)\, (a \,\square\, b) \square\, c = a \,\square\, (\, b \square\, c) = a \,\square\, b \square\, c\,;\ a, b, c \in \mathbb{N};\ \square \in \{\bot, \top\}$
  associativity
- $(\forall a)(\forall b)(\forall c)\, (a \circ b) \circ c = a \circ (b \circ c) = a \circ b \circ c$
  only with
  $a = \dfrac{p^i - q^i}{p - q}\,,\ b = \dfrac{p^j - q^j}{p - q}\,,\ c = \dfrac{p^k - q^k}{p - q}\,;\ p, q, i, j, k \in \mathbb{N};\ p > q\,;\ p \bot q = 1\,;\ i, j | k$
  semiassociativity
- $(\exists !! e)(\forall a)\, a \,\square\, e = e \,\square\, a = a\,;\ e, a \in \mathbb{N}$
  identity property, e – identity element
  $e \bot = \infty\,;\ e \top = 1\,;\ e \circ = 1$

The algebraic structure $(\mathbb{N}; a \,\square\, b)$ is a commutative monoid.
Over and above that the operations $\bot$ and $\top$ obey the laws

- $(\forall a)(\forall b)\, a \bot a = a \top a = a\,;\ a, b \in \mathbb{N}$
  idempotent laws
- $(\forall a)(\forall b)\, a \bot (a \top b) = a \top (a \bot b) = a\,;\ a, b \in \mathbb{N}$
  absorption laws
- $(\forall a)(\forall b)(\forall c)\, (a \bot b) \top c = (a \top c) \bot (b \top c)\,;\ a, b, c \in \mathbb{N}$
  $(\forall a)(\forall b)(\forall c)\, (a \top b) \bot c = (a \bot c) \top (b \bot c)\,;\ a, b, c \in \mathbb{N}$
  distributive laws

The algebraic structure $(\mathbb{N}; a \bot b, a \top b)$ is a distributive lattice, $(\mathbb{N}; a \bot b)$ and $(\mathbb{N}; a \top b)$ are commutative monoids.
The operation $a \circ b$ obeys the following additional laws:

- $(\forall a)\, a \circ a = e \circ = 1$
  involutive law

$(\mathbb{N}; a \circ b)$ is a commutative group with the identity element 1; the inverse a^{-1} is represented by a.

- $a \circ b = \begin{cases} a \cdot b & \text{iff } a \perp b = 1 \\ \frac{a}{b} & \text{iff } a \perp b = b \\ \frac{b}{a} & \text{iff } a \perp b = a \end{cases}$
- $(\forall a)(\forall b)\,(a \cdot a) \circ (a \cdot b) = a \cdot b\,;\ a, b \in \mathbb{N};\ a \perp b = 1$
- $(\forall a)(\forall b)(\forall c)\,(a \boldsymbol{+} b) \bullet c = (a \bullet c) \boldsymbol{+} (b \bullet c)\,;\ a, b, c \in \mathbb{N}$

$a \boldsymbol{+} b$	$a \bullet b$
$a + b$	$a \cdot b$
$a + b$	$a \circ b$
$a \perp b$	$a + b$

- $(\forall a)(\forall b)(\forall c)\,(a \perp b) \circ c = (a \circ c) \top (b \circ c)$
  $(a \top b) \circ c = (a \circ c) \perp (b \circ c)$
  only with
  $a = \dfrac{p^i - q^i}{p - q}\,,\ b = \dfrac{p^j - q^j}{p - q}\,,\ c = \dfrac{p^k - q^k}{p - q}\,;\ p, q, i, j, k \in \mathbb{N};\ p > q\,;\ p \perp q\,;\ i, j | k$
  reverse distributivity

Extension and exhaustion 2

Find a simple and homogeneous algorithm for solving the linear Diophantine equation $\sum_{i=1}^{n} a_i\, x_i = b\,;\ a_i \in \mathbb{N};\ x_i \in \mathbb{Z}\,;\ b \in \mathbb{Z}$ and $\gcd(a_1, a_2, ..., a_n) | b$.

Solution:

Algorithm Diophantine compact

Input: $(a_1, a_2, a_3, ..., a_n)\,;\ b$

$r_1 := a_1\,;\ r_2 := a_2\,;\ r_3 := a_3\,;\ ...\,;\ r_n := a_n$

$i = 2(1)n$

$u := r_{i-1}\,;\ v := r_i\,;\ \underline{w} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

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

$(u, v) := (v, u \bmod v)$

$v = 0$

$r_i := u\,;\ \underline{m}_i := \underline{w}$

$\gcd(a_1, a_2, a_3, ..., a_n) := r_n$

$y_n := \dfrac{b}{\gcd(a_1, a_2, a_3, ..., a_n)}$

$i = n(1)2$

$\begin{pmatrix} y_{i-1} \\ x_i \end{pmatrix} := \underline{m}_i \begin{pmatrix} y_i \\ t_i \end{pmatrix}\,;\ t_i \in \mathbb{Z}$

$x_1 := y_1$

Output: $(x_n, ..., x_3, x_2, x_1)$
$\gcd(a_1, a_2, a_3, ..., a_n)$

Algorithmic idea?

Example 1

$n = 4\,;\ a_1 = 1272\,;\ a_2 = 684\,;\ a_3 = 147\,;\ a_4 = 132\,;\ b = -144$

a_1	a_2	a_3	a_4	$\underline{w}\,,\ \underline{m}_i$
1272	684	147	132	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
684	588			$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}$
588	96			$\begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ -1 & 2 \end{pmatrix}$
96	12			$\begin{pmatrix} 1 & -1 \\ -1 & 2 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -6 \end{pmatrix} = \begin{pmatrix} -1 & 7 \\ 2 & -13 \end{pmatrix}$
12	0			$\begin{pmatrix} -1 & 7 \\ 2 & -13 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -8 \end{pmatrix} = \begin{pmatrix} 7 & -57 \\ -13 & 106 \end{pmatrix} = \underline{m}_2$
	12	147		$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
	147	12		$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
	12	3		$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -12 \end{pmatrix} = \begin{pmatrix} 1 & -12 \\ 0 & 1 \end{pmatrix}$
	3	0		$\begin{pmatrix} 1 & -12 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -4 \end{pmatrix} = \begin{pmatrix} -12 & 49 \\ 1 & -4 \end{pmatrix} = \underline{m}_3$
		3	132	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
		132	3	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
		3	0	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -44 \end{pmatrix} = \begin{pmatrix} 1 & -44 \\ 0 & 1 \end{pmatrix} = \underline{m}_4$
		$\uparrow$		
		$\gcd(a_1, a_2, a_3, a_4)$		

$$y_4 = \frac{b}{\gcd(a_1, a_2, a_3, a_4)} = \frac{-144}{3} = -48$$

$$\begin{pmatrix} y_3 \\ x_4 \end{pmatrix} = \underline{m}_4 \begin{pmatrix} y_4 \\ t_4 \end{pmatrix} = \begin{pmatrix} 1 & -44 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} -48 \\ t_4 \end{pmatrix} = \begin{pmatrix} -48 - 44\,t_4 \\ t_4 \end{pmatrix};\ t_4 \in \mathbb{Z}$$

$$\begin{pmatrix} y_2 \\ x_3 \end{pmatrix} = \underline{m}_3 \begin{pmatrix} y_3 \\ t_3 \end{pmatrix} = \begin{pmatrix} -12 & 49 \\ 1 & -4 \end{pmatrix}\begin{pmatrix} -48 - 44\,t_4 \\ t_3 \end{pmatrix} = \begin{pmatrix} 576 + 528\,t_4 + 49\,t_3 \\ -48 - 44\,t_4 - 4\,t_3 \end{pmatrix};\ t_3 \in \mathbb{Z}$$

$$\begin{pmatrix} y_1 = x_1 \\ x_2 \end{pmatrix} = \underline{m}_2 \begin{pmatrix} y_2 \\ t_2 \end{pmatrix} = \begin{pmatrix} 7 & -57 \\ -13 & 106 \end{pmatrix}\begin{pmatrix} 576 + 528\,t_4 + 49\,t_3 \\ t_2 \end{pmatrix}$$

$$= \begin{pmatrix} 4032 + 3696\,t_4 + 343\,t_3 - 57\,t_2 \\ -7488 - 6864\,t_4 - 637\,t_3 + 106\,t_2 \end{pmatrix};\ t_2 \in \mathbb{Z}$$

Result:

$x_4 = t_4$

$x_3 = -48 - 44\,t_4 - 4\,t_3$

$x_2 = -7488 - 6864\,t_4 - 637\,t_3 + 106\,t_2$

$x_1 = 4032 + 3696\,t_4 + 343\,t_3 - 57\,t_2 \qquad t_2, t_3, t_4 \in \mathbb{Z}$

Check:

$a_1x_1 + a_2x_2 + a_3x_3 + a_4x_4 =$

$1272(4032 + 3696\,t_4 + 343\,t_3 - 57\,t_2) + 684(-7488 - 6864\,t_4 - 637\,t_3 + 106\,t_2)$

$+ 147(-48 - 44\,t_4 - 4\,t_3) + 132(t_4) = -144 = b$

Note:

The algorithm Diophantine compact provides the right results $(x_n, ..., x_3, x_2, x_1)$ also for $\gcd(a_1, a_2, a_3, ..., a_n) \nmid b$, in this case exist $x_i \in \mathbb{Q}$.