Unit n°53

Supplement 3

Given

Linear Diophantine equation with two unknowns x and y

$ax + by = c;$ $\quad a>b;\ a, b \in \mathbb{N}$ (1)

$c \in \mathbb{Z};\quad \gcd(a,b)|c$

$x, y \in \mathbb{Z}$

Example:

$1272x + 684y = -132$ (2.1)

Find

The general solution of eqn.(1) in matrix representation

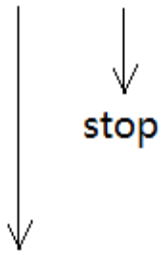
Solution

$\begin{pmatrix} u \\ v \end{pmatrix} := \begin{pmatrix} a \\ b \end{pmatrix};\ \underline{w} := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$		Input : $\begin{pmatrix} a \\ b \end{pmatrix}$
repeat until	$\underline{w} := \begin{pmatrix} 0 & 1 \\ 1 & -\mathrm{div}(u,v) \end{pmatrix} w$	(A1)
	$(u, v) := (v, \mathrm{rest}(u, v))$	
$v=0$		
$\gcd(a, b) := u;\ \underline{n} := \underline{w}^T$		Output: $\gcd(a, b)$; $\underline{n}(a, b)$

$$\begin{pmatrix} x \\ y \end{pmatrix} := \underline{n} \begin{pmatrix} \frac{c}{\gcd(a,b)} \\ t \end{pmatrix};\ t \in \mathbb{Z} \qquad (3)$$

Execution record for the givn example

i	u	v	$\underline{w}$
0	1272	684	$\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}$
1	684	588	$\begin{pmatrix}0 & 1\\1 & -1\end{pmatrix}\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}=\begin{pmatrix}0 & 1\\1 & -1\end{pmatrix}$
2	588	96	$\begin{pmatrix}0 & 1\\1 & -1\end{pmatrix}\begin{pmatrix}0 & 1\\1 & -1\end{pmatrix}=\begin{pmatrix}1 & -1\\-1 & 2\end{pmatrix}$
3	96	12	$\begin{pmatrix}0 & 1\\1 & -6\end{pmatrix}\begin{pmatrix}1 & -1\\-1 & 2\end{pmatrix}=\begin{pmatrix}-1 & 2\\7 & -13\end{pmatrix}$
4	12	0	$\begin{pmatrix}0 & 1\\1 & -8\end{pmatrix}\begin{pmatrix}-1 & 2\\7 & -13\end{pmatrix}=\begin{pmatrix}7 & -13\\-57 & 106\end{pmatrix}$





$\gcd(1272,684) = 12$

$\underline{n}(1272,684) = \begin{pmatrix}7 & -57\\-13 & 106\end{pmatrix}$

$$\begin{pmatrix}x\\y\end{pmatrix}=\begin{pmatrix}7 & -57\\-13 & 106\end{pmatrix}\begin{pmatrix}\frac{-132}{12}\\t\end{pmatrix}=\begin{pmatrix}-77-57t\\143+106t\end{pmatrix} \qquad (2.2)$$

Given

Linear Diophantine equation with two unknowns x and y

$$ax + by + cz + d\omega = e\ ; \qquad a>b>c>d \in \mathbb{N} \qquad (4)$$
$$e \in \mathbb{Z};\quad \gcd(a,b,c,d)\,|\,e$$
$$x, y, z, \omega \in \mathbb{Z}$$

Find

The general solution of eqn.(4) in matrix representation

Nested solution

$$\left.\begin{aligned} &1)\ a, b \xrightarrow{(A1)} \gcd(a, b)\ ,\ \underline{n}_1 \\ &2)\ \gcd(a, b), c \xrightarrow{(A1)} \gcd(a, b, c)\ ,\ \underline{n}_2 \\ &3)\ \gcd(a, b, c), d \xrightarrow{(A1)} \gcd(a, b, c, d)\ ,\ \underline{n}_3 \end{aligned}\right\} \qquad (5)$$

$$\begin{pmatrix} x \\ y \\ z \\ \omega \end{pmatrix} = \underline{n} \begin{pmatrix} \frac{e}{\gcd(a,b,c,d)} \\ r \\ s \\ t \end{pmatrix}\ ;\ r,s,t \in \mathbb{Z} \qquad (6)$$

$$\underline{n} = \begin{pmatrix} \blacksquare & 0 & 0 & \blacksquare \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ \blacksquare & 0 & 0 & \blacksquare \end{pmatrix} \begin{pmatrix} \blacksquare & 0 & \blacksquare & 0 \\ 0 & 1 & 0 & 0 \\ \blacksquare & 0 & \blacksquare & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} \blacksquare & \blacksquare & 0 & 0 \\ \blacksquare & \blacksquare & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \qquad (7)$$

$\underline{n}_3$ $\underline{n}_2$ $\underline{n}_1$

Choose an own example for eqn.(4), calculate the related execution records for eqn.(5) and give the solution eqns.(6) and (7).

Find

Based on this record a compression of the nested solution eqn.(5) into a closed matrix-represented algorithm

$(a,b,c,d,e) \longrightarrow \gcd(a,b,c,d)\ ,\ \underline{n}\ .$