Algorithme d'Euclide matriciel.

I Théorème de Bézout : soient $a, b \in \mathbb{Z}^*$, $\exists u, v \in \mathbb{Z}^*$ / $au + bv = a \wedge b$

1) PGCD(a, b)

$a = bq + r$ avec $0 \leq r < b$

on a $a \wedge b = b \wedge r$

par récurrence, $b = r_0 q_1 + r_1$ $\quad 0 \leq r_1 < r$

on $(b \wedge r_0) = (r_0 \wedge r_1)$ ... $r_1, r_2, \ldots$ suite d'entiers, décroissante.

On en obtient 1 nul.

Le dernier reste non nul est le pgcd.

2) Méthode matricielle.

$a = bq + r$

on cherche π tel que $\begin{pmatrix} b \\ r \end{pmatrix} = \pi \begin{pmatrix} a \\ b \end{pmatrix}$

on pose $b = \frac{a - r}{q}$ et $r = a - bq$

d'où $\begin{pmatrix} b \\ r \end{pmatrix} = \begin{pmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} \alpha_{11} a + \alpha_{12} b \\ \alpha_{21} a + \alpha_{22} b \end{pmatrix} \Rightarrow \pi = \begin{pmatrix} 0 & 1 \\ 1 & -q \end{pmatrix}$

d'où $\begin{pmatrix} b \\ r \end{pmatrix} = \begin{pmatrix} \frac{a-r}{q} \\ a - bq \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}$

3) Ex : trouver u et v tq $d = a \wedge b$

$a = 931$ et $b = 513$ on a $a \wedge b = 19$

$931 = 513 \times 1 + 418$

$\begin{pmatrix} 513 \\ 418 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q \end{pmatrix} \begin{pmatrix} 931 \\ 513 \end{pmatrix}$ avec $q = 1$

$513 = 418 \times 1 + 95$

$$\begin{pmatrix} 418 \\ 95 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 513 \\ 418 \end{pmatrix}$$

$418 = 95 \times 4 + 38$

$$\begin{pmatrix} 95 \\ 38 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -4 \end{pmatrix} \begin{pmatrix} 418 \\ 95 \end{pmatrix}$$

$95 = 38 \times 2 + 19$

$$\begin{pmatrix} 38 \\ 19 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} \begin{pmatrix} 95 \\ 38 \end{pmatrix}$$

et $38 = 2 \times 19 + 0$ fin. d'où $pgcd(931, 513) = 19$

et $\begin{pmatrix} 38 \\ 19 \end{pmatrix} = \prod_{i=1}^{n} Q_i = \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -4 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 931 \\ 512 \end{pmatrix}$

$$\begin{pmatrix} 38 \\ 19 \end{pmatrix} = \begin{pmatrix} 5 & -9 \\ -11 & 20 \end{pmatrix} \begin{pmatrix} 931 \\ 512 \end{pmatrix}$$

La seconde ligne correspond à cette écriture

$19 = -11 \times 931 + 20 \times 512$

II Résolution de $ax = 1 \ (n)$

En class les fractions sont strictement inférieures à l'unité. { dénom : noir / num : gris }

coeff multiplicateur : a - simples pour indiquer que

c'est le reste d'une division par n donc $a < n$

On pose $r_0 = n$, $r_1 = a$

On calcule les "restes" $(r_i)_{1 \le i \le n}$ et les "quotients" $(q_i)_{1 \le i \le n}$

de r_{n-1} par r_n à l'aide de la récurrence $r_{n-1} = r_n q_n + r_{n+1}$

on arrête les divisions quand $r_n = 1$ donc $q_{n-1} = r_{n-1}$

Cela signifie que $n \wedge a = 1$

En fait, on a $\frac{M}{q} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{\cdots + \cfrac{1}{q_n}}}$

La seconde partie de la procédure correspond à déterminer S_n avec $S_0 = 1$ et $S_1 = q_1$, puis le raisonnement "inverse" de celui des entiers.

$$S_{n+1} = q_{n+1} S_n + S_{n-1}.$$

On arrête quand $S_n = M$

La solution propre est alors $x = S_{n-1}$ si n est impair

$x = (r_{n-1} - 1) S_{n-1} + S_{n-2}$ si n est pair.

Ex $5x = 1 \ (7)$

d'où on cherche $\frac{7}{5}$

$7 = 5 \times 1 + 2 \quad q_1 = 1$

$5 = 2 \times 2 + 1 \quad q_2 = 2$

$2 = 2 \times 1 \quad q_3 = 2$

$i =$	0	1	2	3
q_i		1	2	2

Calcul de r_i : • $r_3 = 1$ / on arrête quand $r_n = 1$

$r_2 = q_3$ car $r_n = 1$ alors $r_{n-1} = \underbrace{r_n}_{=1} q_n + \underbrace{r_{n+1}}_{=0}$

$\Rightarrow r_{n-1} = q_n$.

• $r_2 = 2$

• $r_1 = 2 \times 2 + 1 = 5$

• $r_0 = 5 \times 1 + 2 = 7$

i	0	1	2	3
q_i		1	2	2
r_i	7	5	2	1

$S_0 = 1$ et $S_1 = q_1$

$S_2 = q_2 S_1 + S_0 = 2 \times 1 + 1 = 3$

$S_3 = q_3 S_2 + S_1 = 2 \times 3 + 1 = 7$

n est impair $(n=2)$ $x = S_2 = 3$

En notation matricielle, $Q_i = \begin{pmatrix} q_i & 1 \\ 1 & 0 \end{pmatrix}$

$$\begin{pmatrix} r_{i-1} \\ r_i \end{pmatrix} = Q_i \begin{pmatrix} r_i \\ r_{i+1} \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} S_i \\ S_{i-1} \end{pmatrix} = Q_i \begin{pmatrix} S_{i-1} \\ S_{i-2} \end{pmatrix}$$

On a $\begin{pmatrix} M \\ a \end{pmatrix} = \begin{pmatrix} r_0 \\ r_1 \end{pmatrix} = Q_1 \times Q_2 \times \cdots \times Q_n \times \begin{pmatrix} 1 \\ 0 \end{pmatrix}$

$$\begin{pmatrix} S_n \\ S_{n-1} \end{pmatrix} = \begin{pmatrix} M \\ S_{n-1} \end{pmatrix} = Q_n \times Q_{n-1} \times \cdots \times Q_1 \times \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

On obtient $\begin{pmatrix} M \\ S_2 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} * \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 7 \\ 3 \end{pmatrix}$

Comme $n=3$ impair $x = S_2 = 3$ et $3 \times 7 = 2 \times 7 + 1$