

EXEMPLE : PGCD(32, 6)

$$32 = \underbrace{2 \cdot 2 \cdot 2 \cdot 2 \cdot 2}_{} \quad 6 = 3 \cdot \underbrace{2}_{}$$

$$\text{PGCD}(32, 6) = 2$$

$$32x + 6y = 2$$

$$6y = 2 - 32x \Rightarrow y = \frac{1}{3} - \frac{16}{3}x$$

Toute fois on a $x = 3i + 1$ (i.e. $\mathbb{Z}$)

donne un y entier et donc une paire de coeff. de Bézout.

Rappel : Le théorème de Bachet-Bézout nous donne l'existence des coefficients de Bézout de la forme

$$\text{PGCD}(a, b) = a \cdot x + b \cdot y \quad a, b, x, y \in \mathbb{Z} \\ a, b \text{ non nuls.}$$

Algorithme d'Euclide ETENDU

Entrée : a et b deux entiers $\mathbb{Z}^*$ ($a \geq b$)

Sortie : PGCD(a, b) ET les coeff de Bézout x et y tels que

$$\text{PGCD}(a, b) = a \cdot x + b \cdot y$$

EXEMPLE: $\text{PGCD}(168, 32)$

Euclide Classique	$\begin{array}{l} \text{INSTR.} \\ \vdots \end{array}$	$r_0 = 168$	$x_0 = 1$	$y_0 = 0$	$\left. \begin{array}{l} \\ \\ \end{array} \right\} \text{FIXE}$
		$r_1 = 32$	$x_1 = 0$	$y_1 = 1$	

Euc. de Clastique

$$\begin{array}{l} \text{1. } r_0 = 168 \quad x_0 = 1 \quad y_0 = 0 \\ r_1 = 32 \quad x_1 = 0 \quad y_1 = 1 \end{array} \quad \left. \vphantom{\begin{array}{l} r_0 = 168 \\ r_1 = 32 \end{array}} \right\} \text{F.T.X.E}$$

Etape 2

$$\begin{array}{r} 168 \overline{) 32} \\ 8 \overline{) 5} \end{array} \quad q_2 = 5$$

$$\begin{aligned} r_2 &= 8 \\ x_2 &= x_0 - q_2 \cdot x_1 = 1 - 5 \cdot 0 = 1 \\ y_2 &= y_0 - q_2 \cdot y_1 = 0 - 5 \cdot 1 = -5 \end{aligned}$$

Etape 3

$$\begin{array}{r} 32 \overline{) 8} \\ 4 \overline{) 0} \end{array} \quad q_3 = 4$$

$$\begin{aligned} r_3 &= 0 \\ x_3 &= x_1 - q_3 \cdot x_2 = 0 - 4 \cdot 1 = -4 \\ y_3 &= y_1 - q_3 \cdot y_2 = 1 - 4 \cdot (-5) = 21 \end{aligned}$$

Si $r_k = 0$, alors $\text{PGCD}(168, 32) = r_{k-1} = 168 \cdot x_{k-1} + 32 \cdot y_{k-1}$
 dernier reste non-nul

Exemples

$$\begin{array}{l} \text{Ex. 0} \\ \text{Ex. 1} \end{array} \quad \begin{array}{l} r_0 = a \quad x_0 = 1 \quad y_0 = 0 \\ r_1 = b \quad x_1 = 0 \quad y_1 = 1 \end{array}$$

Etape i

$$\begin{array}{r} r_{i-2} \overline{) r_{i-1}} \\ r_i \overline{) q_i} \end{array}$$

$$\begin{aligned} x_i &= x_{i-2} - q_i \cdot x_{i-1} \\ y_i &= y_{i-2} - q_i \cdot y_{i-1} \end{aligned}$$

Exercice : Calculez le PGCD ET les coeff. De Bézout de $a = 720$ et $b = 504$.

$$r_0 = 720 \quad x_0 = 1 \quad y_0 = 0$$

$$r_1 = 504 \quad x_1 = 0 \quad y_1 = 1$$

$$\begin{array}{r} 720 \overline{) 504} \\ 216 \overline{) 7} \end{array} \quad q_2 = 7$$

$$\begin{aligned} r_2 &= 216 \\ x_2 &= x_0 - q_2 \cdot x_1 = 720 - 7 \cdot 504 = 216 \\ y_2 &= y_0 - q_2 \cdot y_1 = 0 - 7 \cdot 1 = -7 \end{aligned} \quad \left. \vphantom{\begin{array}{l} r_2 = 216 \\ x_2 = 216 \end{array}} \right\} 216 = 720 \cdot 1 + 504 \cdot (-1)$$

$$\begin{array}{r} 504 \overline{) 216} \\ 72 \overline{) 2} \end{array} \quad q_3 = 7$$

$$\begin{aligned} r_3 &= 72 \\ x_3 &= x_1 - q_3 \cdot x_2 = 0 - 7 \cdot 216 = -1512 \\ y_3 &= y_1 - q_3 \cdot y_2 = 1 - 7 \cdot (-7) = 50 \end{aligned}$$

$$\begin{array}{r} 216 \overline{) 72} \\ 0 \overline{) 3} \end{array} \quad q_4 = 3$$

$$r_4 = 0 \quad \boxed{\text{STOP}}$$

Réponse: $\text{PGCD}(770, 504) = 72 = 770 \cdot (-2) + 504 \cdot 3$

Astuces:

1. $x_2 = 1$ $y_2 = -q_2$ Toujours !!!!
2. A chaque étape i , x_i et y_i sont de signe INVERSE !!!!
3. A chaque étape i , on a l'égalité suivante

$$r_i = a \cdot x_i + b \cdot y_i$$

Exercice de pause : PGCD et coeff. de Bézout pour $a=612$ et $b = 208$?

Réponse : $\text{PGCD}(612, 208) = 4 = 612 \cdot 17 + 208 \cdot (-50)$

Arithmétique Modulaire Gauss (1801)

Définition : l'opérateur MODULO : $a \bmod N = r$ si

$$a = q \cdot N + r \quad \text{où} \quad a, q, N \text{ et } r \in \mathbb{Z}$$

$$\text{et } r \in [0, \dots, N-1]$$

$$N \geq 1$$

Si on récrit cela avec la division euclidienne

$$\begin{array}{r|l} a & N \\ \hline r & q \end{array} \quad a \bmod N = r$$

Exemples: calculez

$$11 \bmod 2 = 1 = (\underline{5} \cdot 2 + 1) \bmod 2$$

$$2 \bmod 11 = 2 = (\underline{0} \cdot 11 + 2) \bmod 11$$

$$-2 \bmod 11 = 9 = [1 \cdot 11 + (-2)] \bmod 11 = (0 \cdot 11 + 9) \bmod 11$$

$$-11 \bmod 11 = 0$$

$$\left[\begin{array}{c|c} -11 & 1 \\ \hline 0 & -11 \end{array} \right]$$

Notations : $a \bmod N = b$

$$(a \% N = b)$$

CONGRUENCE:

a est congruent à b modulo N si $a \bmod N = b \bmod N$,

On le note $a \equiv_N b$.

NOTE: si a ET b sont dans $[0, N-1]$

Alors $a \equiv_N b$ implique que $a = b$!

$$11 \equiv_{10} 21 \equiv_{10} 1 \equiv_{10} -9$$

$$1 \equiv_{10} 1 \Rightarrow \boxed{1=1}$$



$$-9 \equiv_{10} 11 \text{ ok}$$

$$-1 = 11 \text{ PAS VRAI}$$

Si $a \equiv_N b \Rightarrow \left. \begin{array}{l} a = q_1 \cdot N + r \\ \text{et } b = q_2 \cdot N + r \end{array} \right\} \begin{array}{l} \text{c'est le même reste} \\ \text{si } r \in [0, N-1] \end{array}$

Si $a \bmod N \in [-N+1, \dots, N-1]$

$$a \equiv_N b \text{ si } \left\{ \begin{array}{ll} a \bmod N = b \bmod N & (\text{même signe}) \\ a \bmod N + N = b \bmod N & (a \bmod N < 0, b \bmod N > 0) \\ a \bmod N = b \bmod N & (a \bmod N > 0, b \bmod N < 0) \end{array} \right.$$

Série 7 Ex 1:

Ensembles disjoints $\Rightarrow$ Aucun élément en commun !

$a \in \mathbb{Z} \Rightarrow a \bmod N = r \in [0, \dots, N-1]$
 donc $a \in E_r$ par définition } prouve que les E_i
 couvrent tous les $\mathbb{Z}$

Disjoint: 2 E_i, E_j n'at jamais d'élément commun

Absurde: Supposons qu'il existe a tel que $\underbrace{a \in E_i}_{\text{red}} = \underbrace{a \in E_j}_{\text{green}}$
 avec $i \neq j$!

$a = q_a \cdot N + i$ $i \in [0, \dots, N-1]$

$a = q_b \cdot N + j$

$a \equiv_N a \equiv_N i$ $\swarrow$ car $a \in E_i$
 $\equiv_N j$ $\nwarrow$ car $a \in E_j$

EGALITE SI i et $j \in [0, \dots, p-1]$
 $i \equiv_N j$

avec $i \in [0, \dots, p-1]$
 $j \in [0, \dots, N-1]$

$\Downarrow$
 $\boxed{i=j \quad !}$

Contredit $i \neq j$!

Cela prouve que le reste de la division entière est UNIQUE !