

Relat° de Bézout pour une paire $(a, b) \in \mathbb{Z}^{*2}$ est une écriture:

$$ax + by = \text{pgcd}(a, b)$$

Exercice 4.5. Déterminer une relation de Bézout pour les paires d'entiers $(17, 27)$, $(168, 245)$ et $(128, 320)$.

$$27 = 17 \times 1 + 10$$

$$17 = 10 \times 1 + 7$$

$$10 = 7 \times 1 + 3$$

$$7 = 3 \times 2 + 1 \quad \text{pgcd}(27, 17) = 1$$

$$3 = 1 \times 3 + 0$$

$$245 = 168 \times 1 + 77$$

$$168 = 77 \times 2 + 14$$

$$77 = 14 \times 5 + 7 \quad \text{pgcd}(245, 168) = 7$$

$$14 = 7 \times 2 + 0$$

$$7 = 77 - 14 \times 5$$

$$= 77 - 168 + 77 \times 2 = 77 \times 3 - 168$$

$$= (245 - 168 \times 1) \times 3 - 168$$

$$= 245 \times 3 - 4 \times 168 = 7$$

$$320 = 128 \times 2 + 64 \quad \text{pgcd}(320, 128) = 64$$

$$128 = 64 \times 2 + 0$$

$$64 = 320 - 128 \times 2$$

$$(21, 38)$$

$$38 = 21 \times 1 + 17$$

$$21 = 17 \times 1 + 4$$

$$17 = 4 \times 4 + 1$$

$$4 = 1 \times 4 + 0$$

$$1 = 17 - 4 \times 4$$

$$= 17 - (21 - 17 \times 1) \times 4$$

$$= -3 \times 17 + 4 \times 21$$

$$= -3 \times (38 - 21 \times 1) + 4 \times 21$$

...

Exercice 4.6. (1) Soit $a = 132$, $b = 60$ et $d = \text{pgcd}(132, 60)$.

(a) Factoriser a et b en produit de nombres premiers et donner la valeur de d .

$$132 = 2 \times 66 = 2^2 \times 3 \times 11 = 2^2 \times 3 \times 11$$

$$60 = 2^2 \times 3 \times 5$$

$$\text{pgcd}(132, 60) = 12$$

(b) Retrouver d à l'aide de l'algorithme d'Euclide et en déduire une paire d'entiers (x_0, y_0) tels que $132x_0 + 60y_0 = d$.

$$132 = 60 \times 2 + 12$$

$$60 = 12 \times 5 + 0.$$

$$2 \times 132 - 60 \times 4.$$

$$12 = 132 - 60 \times 2, \quad x_0 = 1, y_0 = -2.$$

(c) Pour $c \in \mathbb{Z}$, posons $S_c = \{(x, y) \in \mathbb{Z}^2 : ax + by = c\}$. Déterminer S_c dans chacun des cas suivants.

(i) $c = d$;

(ii) $c = d + 1$;

(iii) $c = 10d$.

Cours : Équations diophantiennes.

pb1: Soient $(a, b) \in \mathbb{Z}^{*2}$

Déterminer toutes les relat° de Bézout pour a et b .

$$(E1) \quad ax + by = d \text{ avec } d = \text{pgcd}(a, b).$$

$$a' = \frac{a}{d}, \quad b' = \frac{b}{d}$$

Pas rappel S: $m|a$ et $m|b$ alors:

$$\text{pgcd}\left(\frac{a}{m}, \frac{b}{m}\right) = \frac{\text{pgcd}(a, b)}{m}$$

$$\text{On a alors: } \text{pgcd}(a'; b') = \text{pgcd}\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{\text{pgcd}(a, b)}{d} = \frac{d}{d} = 1.$$

en divisant (E1) par d , il vient que

(E2): $a'x + b'y = 1$, est une relation de Bézout donnée par l'algo d'Euclide.

$$(E3): a'x + b'y = a'x_0 + b'y_0 \Leftrightarrow a'(x - x_0) = b'(y - y_0)$$

$$\text{Comme: } \left. \begin{array}{l} b' | a'(x - x_0) \\ \text{pgcd}(a', b') = 1 \end{array} \right\} \Rightarrow b' | x - x_0.$$

$\exists k \in \mathbb{Z}, x - x_0 = kb'$ Donc (E3) devient

$$a'(kb') = b'(y - y_0) = -a'k = y - y_0.$$

Les solut^o de (E1) sont:

$$S = \{(x, y), x - x_0 = kb', y - y_0 = -ka', k \in \mathbb{Z}\}$$

Pb2.

Résoudre $ax + by = c$ où $(x, y) \in \mathbb{Z}^2$. (E4)

Théorème 2:

(E4) admet une solut^o $\Leftrightarrow \text{pgcd}(a, b) \mid c$.

Supposons que $\text{pgcd}(a, b) \mid c \equiv d \mid c$.

On pose $c' = \frac{c}{d}$. En divisant (E4) par d , il vient que:

$$(E5): a'x + b'y = c'$$

$$\Leftrightarrow a'x + b'y = c'(a'x_0 + b'y_0) \text{ car } a'x_0 + b'y_0 = 1.$$

$$a'(x - cx_0) = b'(y - cy_0). \quad b' \mid a'(x - cx_0) \text{ (car } b' \mid a')$$

$$\Rightarrow \exists k \in \mathbb{Z}, x - cx_0 = kb'$$

$$(E5) \text{ devient: } a'kb' = b'(y - cy_0) \quad (E6)$$

$$\Rightarrow y - cy_0 = -ka'.$$

L'ensemble des solut^o de (E4) est donc:

$$S = \{(x, y), x - cx_0 = kb' \text{ et } y - cy_0 = -ka'\}.$$

