5 équations $ax+by=c$; $(x,y)\in\mathbb{Z}^2$

Soit $(a,b)\in\mathbb{Z}\times\mathbb{Z}$, on cherche à résoudre dans $\mathbb{Z}\times\mathbb{Z}$ l'équation $ax+by=c$;

Soit $d=\text{pgcd}(a,b)$

Remarque : $d\mid a$ et $d\mid b$ donc $d\mid ax+by$ i.e. $d\mid c$; on en déduit le résultat suivant : si $d\nmid c$; l'équation $ax+by=c$ ne possède aucune solution

Supposons maintenant que $d\mid c$ et voyant comment résoudre concrètement cette équation.

On choisit un exemple :

$$931x+513y=c.$$

$\text{pgcd}(931,513)=19.$

si c n'est pas un multiple de 19 pas de solution

si $c=19c'$, $c'\in\mathbb{Z}$ l'équation devient : $49x+27y=c'$.

L'algorithme d'euclide donne l'identité de Bezout

(1) $49\times(-11)+27\times20=1$

$(x_0, y_0) = (-11c', 20c')$ est une solution particulière

$$49x + 27y = c' = 49 \times x_0 + 27 y_0$$

Ce qui donne : $49(x - x_0) = 27(y_0 - y)$.

$27 \mid 49(x - x_0)$, $(27, 49) = 1$ on obtient

par le lemme de Gauss : $27 \mid x - x_0$ ou encore

$$x - x_0 = 27k \Rightarrow x = 27k + x_0.$$

En le reportant dans l'équation, on obtient.

$$\cancel{49} \quad 27(y_0 - y) = 49 \times 27k$$

ou encore $y_0 - y = 49k$, $y = y_0 - 49k$.

$x = 27k + x_0$ et $y = y_0 - 49k$, on vérifie que (x, y)

est solution de l'équation.

En conclusion : les solutions sont $(-11c' + 27k, 20c' - 49k)$

$k \in \mathbb{Z}$.

- PPCM Soit (a, b) deux entiers ;

On note $\text{ppcm}(a, b)$ le plus petit entier positif multiple de a et de b

On suppose pour simplifier sans perdre de généralité que a, b sont positifs.

ab est un multiple de a et de b, ce n'est cependant pas le plus ~~petit~~ petit.

Soit $d = \text{pgcd}(a, b)$; on peut écrire

$a = da'$, $b = db'$, avec (a', b') premiers entre eux. L'entier $da'b'$ est un ~~nu~~ multiple a et aussi de b car on peut l'écrire ba'.

c'est donc un multiple de a et de b, on voit bien qu'il est plus petit que ab. ($ab = d^2a'b'$).

En fait on a ~~le résultat~~ théorème suivant:

th: $\text{PPCM}(a, b) = da'b'$.

<u>preuve</u>: Soit $m = \text{PPCM}(a, b)$

$m = ak = da'k$; $b = db'$

$b \mid m \Leftrightarrow db' \mid da'k \Rightarrow b' \mid a'k$

or $(b', a') = 1 \Rightarrow b' \mid k$, Ainsi: $k = b'k'$

$m = ak = da'k = da'b'k'$.

On en tire: $\underbrace{da'b'}_{\text{multiple commun de } (a,b)} \mid m \Rightarrow da'b' = m$.

Remarque : si $(a,b) = 1 \Rightarrow PPCM(a,b) = ab$

réciproquement si $PPCM(a,b) = ab \Rightarrow$

$$ab = d^2 a' b' = d a' b \Rightarrow d = 1$$

i.e. $(a,b) = 1$

Corollaire : (a,b) entiers naturels :

$$\boxed{ab = pgcd(a,b)\, ppcm(a,b)}$$

Exemple : $a = 931$, $b = 513$.

$d = pgcd(a,b) = 19$.

$$ppcm = \frac{931 \times 513}{19} = \frac{49 \times 19 \times 27 \times 19}{19}$$

$$= 49 \times 27 \times 19$$