I/ Théorème fondamental de l'arithmétique

TR : $\forall N \in \mathbb{Z}$ $\exists !$ liste de nb premiers $p_1, \dots, p_k$ et $\exists !$ liste d'entiers $m_1, \dots, m_k > 0$ tq $N = p_{m_1}^{m_1} \cdot p_2^{m_2} \cdots p_k^{m_k}$

Démonstration

* *init :* $N = 2$ $\Rightarrow$ OK

* *hérédité :* Supposons que c'est vrai pour $2, 3, \dots, n-1$

  · Soit n est premier $\Rightarrow$ OK

  · Soit n n'est pas premier.
  Alors il existe $1 < a, b < n$ tq $n = a \times b$
  Par hypothèse de récurrence, a et b admettent une décomposition en facteurs premiers.
  Donc n aussi.

Voir le poly pour la preuve d'unicité.

TR : Il existe une infinité de nb premiers

Démonstration :
Par l'absurde.
Supposons qu'il en existe un nb fini : $\{p_1, \dots, p_n\}$, $n \in \mathbb{N}$

Soit $N = p_1 p_2 \dots p_n + 1$

Soit q un nb premier qui divise N.

Si $q = p_i$ pour un certain i. $q \mid N$ par hypothèse et $q \mid N-1$

donc $q \mid N - (N-1) \Rightarrow q \mid 1$ absurde

$q \notin \{p_1, \dots, p_n\}$ $\Rightarrow$ il existe une infinité de nombres premiers

II/ Applicatⁿ de Bezout pour résoudre des Equations.

But : résoudre $ax + by = c$, $a, b, c \in \mathbb{Z}$

· Si a ou $b = 0$ $\Rightarrow$ trivial

· On suppose a et $b \neq 0$
Soit $d = PGCD(a, b)$
Alors $d \mid a$ et $d \mid b$
Donc $\forall (x, y) \in \mathbb{Z}^2$, $d \mid ax + by$ donc $d \mid c$ si (x, y) est une solution.

Règle n°1 : Si d ne divise pas c $\Rightarrow$ PAS DE SOLUTION

Supposons $d \mid c$, $\exists c' \in \mathbb{Z}$ tq $c = dc'$

TR de Bezout : $\exists (u, v) \in \mathbb{Z}$ tq $au + bv = d$ $\Rightarrow$ $a(uc') + b(vc') = dc' = c$

Autrement dit : on pend $d' = \frac{a}{d}$ et $b' = \frac{b}{d}$

L'équation de départ a les mêmes solutions que $a'x + b'y = c'$ et ici a' et b' sont premiers entre eux.

On a une solution particulière $(u_0, v_0) = (c'u, c'v)$

Soient (x_1, y_1) une autre solution.

En soustrayant, on voit que $a'(x_1 - x_0) + b'(y_1 - y_0) = 0$

Comme a' et b' sont premiers entre eux, par le lemme de Gauss $a' \mid (y_1 - y_0)$

$\exists k \in \mathbb{Z}$ tq $-(y_1 - y_0) = a'k$

En remplaçant $a'(x_1 - x_0) = b'a'k$

$\Leftrightarrow \quad (x_1 - x_0) = b'k$

Règle 2 : Si (x_0, y_0) est une solution particulière de $ax + by = c$ $(*)$ et si $d = PGCD(a, b)$

Alors l'ensemble des solutions de $(*)$ sont $\left\{ x_0 + \frac{bk}{d}, y_0 - \frac{ak}{d} \right\}, k \in \mathbb{Z}$

Ex : 1) $102x + 38y = 47$

2) $102x + 38y = 100$

1) PGCD
$102 = 2 \times 38 + 26$
$38 = 1 \times 26 + 12$
$26 = 2 \times 12 + 2$
$12 = 2 \times 6 + 0$

$PGCD(102, 38) = 2 \nmid 47$ donc pas de solution

2) $2 \mid 100$ donc solutions

On commence par calculer Bezout

$2 = 26 - 2 \times 12$
$= 26 - 2 \times (38 - 1 \times 26)$
$= 3 \times 26 - 2 \times 38$
$= 3 \times (102 - 2 \times 38) - 2 \times 38$
$= 3 \times 102 + (-8) \times 38$

$\times 50 \rightarrow \quad 100 = 150 \times 102 + (-400) \times 38$

$(x_0, y_0) = (150, -400)$

$\left(150 + \underset{\uparrow 38/2}{19}k, -400 - \underset{\uparrow 102/2}{51}k\right), k \in \mathbb{Z}$ est l'ensemble des solutions de 2)