Khôlles de Mathématiques - Semaine 17

Kylian Boyet

4 Février 2024

4 Théorème de Bézout

Soient $a, b \in \mathbb{N}^*$ et $c \in \mathbb{Z}$. Il existe des entiers $x, y \in \mathbb{Z}$ tels que $ax + yb = c$ si et seulement si c est multiple du pgcd de a et b.

Démonstration. Soient $a, b \in \mathbb{N}^*$. On suppose l'algorithme d'Euclide réalisé pour a, b, ainsi à la fin de ce dernier on a un entier naturel r_n tel que $r_n = a \wedge b$. Comme l'algorithme est terminé, on peut remonter chaque ligne de proche en proche, on aurait, à titre d'exemple, pour une première itération, $r_n = r_{n-2} - q_n \cdot r_{n-1}$. En réalisant toutes les étapes nécessaires, on obtient une relation entre r_n et a, b, cette relation s'écrit :

$$\exists\ (x_0, y_0) \in (\mathbb{Z}^*)^2\ :\ a \wedge b = r_n = ax_0 + y_0 b.$$

Si c est un multiple de $a \wedge b$, alors il existe $k \in \mathbb{Z}^*$ tel que $c = k(a \wedge b)$, donc en multipliant le résultat montré au dessus par k, on a le sens indirect. Si pour $c \in \mathbb{Z}$, il existe des entiers $x, y \in \mathbb{Z}$ tels que $ax + yb = c$, alors le pgcd de a et b divise le membre de gauche et donc par égalite le membre de droite aussi donc c est multiple de $a \wedge b$, ce qui suffit. □

6 Théorème de Gauss

Soient a, b, c trois entiers naturels non nuls. Si c est premier avec a et divise le produit ab, alors il divise b.

Démonstration. Soient a, b, c des entiers naturels vérifiant les hypothèses.
Comme c est premier avec a on écrit une relation de Bézout pour 1, leur pgcd et on multiplie le tout par b :

$$\exists\ (u, v) \in (\mathbb{N}^*)^2\ :\ au + vc = 1 \implies abu + vbc = b,$$

or c divise ab et lui-même donc aussi le membre de gauche donc par égalité, le membre droite, c'est le théorème. □

8 Résoudre une équation du type $ax + yb = c$

Soient $a, b, c \in \mathbb{Z}$. Résoudre l'équation

$$ax + yb = c,$$

d'inconnues x et y dans $\mathbb{Z}$.

Démonstration. Soient $a, b, c \in \mathbb{Z}$ et une telle équation, notée (i), en lesdites inconnues.
Si $a \wedge b \not| c$, alors le théorème de Bézout, affirme que l'équation n'a pas de solution.
Supposons le contraire. Posons $d = a \wedge b$. Le lemme technique affirme l'existence de a' et b' dans $\mathbb{Z}$, tels que $a'd = a$, $b'd = b$ et $a' \wedge b' = 1$. Donc, comme d divise c, il existe c' tel que $c = c'd$. On réécrit l'équation, notée (ii) :

$$a'x + yb' = c'.$$

On sait d'après le théorème de Bézout qu'il existe des solutions, en particulier grâce à l'algorithme d'Euclide on construit (x_0, y_0), une solution de la nouvelle équation, puis on l'injecte et on raisonne par équivalence, on note ω l'ensemble des solutions de (ii) et Ω celui de (i) :

$$
\begin{array}{lll}
(x,y) \in \Omega & \iff & (x,y) \in \omega \\
& \iff & a'x + yb' = c' \\
& \iff & a'x + yb' = a'x_0 + y_0 b' \\
& \iff & a'(x - x_0) = b'(y_0 - y) \\
& \iff & \exists\, k \in \mathbb{Z} \ : \left\{ \begin{array}{rcl} a'(x - x_0) & = & b'(y_0 - y) \\ y_0 - y & = & a'k \end{array} \right. \\
& \iff & \exists\, k \in \mathbb{Z} \ : \left\{ \begin{array}{rcl} a'(x - x_0) & = & b'(y_0 - y) \\ y & = & y_0 - a'k \end{array} \right. \\
& \iff & \exists\, k \in \mathbb{Z} \ : \left\{ \begin{array}{rcl} x & = & x_0 + b'k \\ y & = & y_0 - a'k \end{array} \right. \\
& \iff & (x,y) \in \{(x_0 + b'k,\ y_0 - a'k) \mid k \in \mathbb{Z}\}
\end{array}
$$

La première ligne découle de la divisibilité des coefficients par d, la deuxième est la définition d'appartenance à ω, la troisième est une réécriture du fait que (x_0, y_0) soit solution de (ii), la quatrième est une factorisation banale, la cinquième une utilisation du théorème de Gauss pour le sens direct et le sens indirect ne pose pas de problème, la sixième est une réécriture de la deuxième relation, la septième découle de l'expression de y pour le sens direct et le sens indirect s'obtient en multipliant avec parcimonie l'équation, la huitième est une réécriture de la septième qui ne pose pas de problème. C'est Ω, par équivalence.

□