Pôle Universitaire Léonard de Vinci
CS 102 – Mathématiques pour l'informatique

S1 – Année 2005-2006
Promotion ESILV 2010

Le théorème de Bézout

Résolution d'une équation diophantienne

Théorème

Soit p et q deux entiers premiers entre eux, c'est-à-dire dont le plus grand commun diviseur (PGCD) est 1. Il existe au moins deux entiers m et n tels que $mp + nq = 1$.

Exemple

Les entiers 25 et 9 sont premiers entre eux, en appliquant le théorème de Bézout[1], on peut trouver au moins deux entiers m et n tels que $mp + nq = 1$. On a, par exemple, $4 \times 25 - 9 \times 9 = 1$.

Démonstration

Notons

$$E = \{mp + nq,\ (m, n) \in \mathbb{Z}^2\}$$

L'ensemble $E \cap \mathbb{N}^*$ est minoré, il admet donc un plus petit élément que nous noterons d. Comme d est un élément de E, il existe deux entiers m et n tels que $d = mp + nq$, en outre d est dans $\mathbb{N}^*$ donc

$$d = mp + nq > 0$$

La division entière de p par d donne $p = ds + r$ où s et r sont des entiers et $0 \leq r < d$. L'entier r est donné par

$$\begin{aligned} r &= p - ds \\ &= p - (mp + nq)s \\ &= (1 - ms)p + (-ns)q \end{aligned}$$

donc r est un élément de E. Or d est le plus petit élément de $E \cap N^*$ donc l'appartenance de r à E entaine $r = 0$. Par suite $p = ds$ donc d divise p.

De manière analogue, la division entière de q par d donne que d divise q. Ainsi d divise p et q. Or p et q sont premiers entre eux, donc $d = 1$. Ainsi 1 appartient à E et donc il existe deux entiers m et n tels que $mp + nq = 1$. CQFD.

Remarque : cette démonstration doit vous rappeler une démonstration du cours.

[1] Etienne Bézout, mathématicien français du XVIIIe siècle, publia en 1779, *Théorie générale des équations algébriques* dans laquelle il s'interesse aux systèmes d'équations polynomiales, et les relations entre les coéficients d'un polynôme et ses racines.

Etienne Bézout (1730–1783)

Algorithme

On utilise plusieurs fois la division euclidienne et on “remonte” vers l’équation de départ. Par exemple

$$\begin{aligned} 25 &= 9 \times 2 + 7 \\ 9 &= 7 \times 1 + 2 \\ 7 &= 2 \times 4 + 1 \end{aligned}$$

On s’arrete puisque le reste est 1 (c’est le PGCD de 25 et 7). On “remonte” :

$$\begin{aligned} 1 &= 7 - 2 \times 3 \\ 1 &= 7 - (9 - 7 \times 1) \times 3 \\ 1 &= 7 \times 4 - 9 \times 3 \\ 1 &= (25 - 9 \times 2) \times 4 - 9 \times 3 \\ 1 &= 25 \times 4 - 9 \times 11 \end{aligned}$$

ce qui donne le résultat.

Equations Diophantienne

Equations Diophantienne est le nom donné aux équations polynomiales de variables entières. Dans le cas général elles sont difficiles à resoudre, voire même impossible : en 1970, Yuri Matiyasevich prouva qu’il existe des équations Diophantienne non résoluble. La célèbre conjecture de Fermat : pour n entier supérieur ou égal à 3, il n’existe pas d’entiers x, y et z tels que $x^n + y^n = z^n$ est une équation Diophantienne, elle fut très longtemps sans démonstration. Il fallu attendre la fin du XXe siècle pour qu’Andrew Wiles apporte une preuve à cette conjecture.