Arithmétique – Partie 2 : Théorème de Bézout

Savoir.

- ☐ Connaître le théorème de Bézout.
- ☐ Comprendre ce que sont les nombres premiers entre eux.
- ☐ Connaître le lemme de Gauss.

Savoir-faire.

- ☐ Savoir calculer les coefficients de Bézout par remontée de l'algorithme d'Euclide.

Le théorème de Bézout

Théorème de Bézout. Soient a et b deux entiers positifs et $d = \text{pgcd}(a, b)$. Alors il existe deux entiers u et v tels que :

$$\boxed{au + bv = d}$$

Les coefficients de Bézout

Les entiers u et v de ce théorème (souvent appelés *coefficients de Bézout*) ne sont pas uniques ! Loin s'en faut... Mais on peut tout de même parvenir à déterminer un couple (u, v) convenable grâce à l'algorithme d'Euclide. C'est d'ailleurs sur cet algorithme que repose la preuve du théorème.
Nous allons expliquer la méthode sur un exemple. On a vu dans les exemples précédents que $\text{pgcd}(1\,188, 120) = 12$. Déterminons des entiers u et v tels que $1\,188u + 120v = 12$. La méthode consiste à "remonter" l'algorithme d'Euclide en exprimant, à partir du pgcd (qui est le dernier reste non nul), chaque reste comme une différence impliquant le dividende et le quotient.

Pour les calculs suivants il faut d'abord lire la colonne de gauche de haut en bas (qui n'est rien d'autre que l'algorithme d'Euclide), puis remonter la colonne de droite de bas en haut (afin de déterminer les coefficients de Bézout u et v).

$$\begin{array}{rcl}
1\,188 = 120 \times 9 + {\color{blue}108} & \rightarrow & \boxed{12} = 120 - {\color{blue}108} = 120 - (1\,188 - 120 \times 9) \\
 & & \quad = 1\,188 \times (-1) + 120 \times 10 \\
120 = 108 \times 1 + \boxed{12} & \rightarrow & \boxed{12} = 120 - 108 \times 1 = 120 - 108
\end{array}$$

Ainsi on a $1\,188 \times (-1) + 120 \times 10 = 12$.

Exercice.

- Déterminer des entiers u et v tels que $585u + 247v = 13$.
- Déterminer des entiers u et v tels que $121u + 73v = 5$.

Nombres premiers entre eux

- Deux entiers a et b sont dits **premiers entre eux** si $\text{pgcd}(a, b) = 1$. Cela signifie que a et b n'ont aucun diviseur en commun autre que 1.
- **Variante du théorème de Bézout.**

$$\boxed{a \text{ et } b \text{ sont premiers entre eux} \iff \text{il existe } (u, v) \in \mathbb{Z}^2 \text{ tels que } au + bv = 1}$$

— *Démonstration.* Il s'agit d'un emploi du théorème de Bézout. Si $\text{pgcd}(a, b) = 1$, alors le théorème de Bézout assure l'existence des entiers u et v tels que $au + bv = 1$.
Réciproquement si $au + bv = 1$, considérons d un diviseur commun à a et à b. $d|a$ et $d|b$ donc $d|au + bv$ et donc $d|1$! Le seul diviseur commun à a et b est donc 1, ce qui signifie qu'ils sont premiers entre eux.

— *Exercice.* Sachant que $83 \times 11 - 24 \times 38 = 1$, détermine quatre couples d'entiers qui sont premiers entre eux.

— *Exercice.* Dans chaque cas, explique si tu peux trouver des entiers u et v tels que $au + bv = 1$ et si c'est le cas trouve-les effectivement :
  - $a = 1\,498$ et $b = 1\,122$
  - $a = 331$ et $b = 82$
  - $a = 17\,802$ et $b = 11\,043$

— Donnons un exemple d'utilisation un peu plus théorique de cette identité de Bézout en montrant que pour tout $n \in \mathbb{Z}$:
$$\text{pgcd}(2n + 3, 5n + 7) = 1.$$
En d'autres termes, les nombres $2n + 3$ et $5n + 7$ sont toujours premiers entre eux, quelle que soit la valeur de l'entier n.
Le but ici est de déterminer une identité de Bézout, c'est-à-dire de trouver des nombres u et v tels que $(2n + 3)u + (5n + 7)v = 1$. Pour cela, on cherche donc à éliminer le nombre n : prenons $v = -2$ et $u = 5$, cela donne :
$$(2n + 3) \times 5 + (5n + 7) \times (-2) = 10n + 15 - 10n - 14 = 1$$
D'après le théorème de Bézout, on a bien $\text{pgcd}(2n + 3, 5n + 7) = 1$.

Lemme de Gauss

Voici une application importante du théorème de Bézout.
Lemme de Gauss. Soient trois entiers non nuls a, b, c.

$$\boxed{\text{Si } a|bc \text{ et } \text{pgcd}(a, b) = 1, \text{ alors } a|c}$$

Démonstration. Puisque $a|bc$, il existe $k \in \mathbb{Z}$ tel que $bc = ka$. D'autre part, d'après le théorème de Bézout on a $au + bv = 1$. On multiplie l'égalité de Bézout par c : $auc + bcv = c$. Puis on remplace bc par ka : $auc + kav = c$. Ainsi $a(uc + kv) = c$ c'est-à-dire $a|c$.

Corollaire. Si a et b divisent c et $\text{pgcd}(a, b) = 1$, alors $ab|c$.
Démonstration. On sait que $c = ka = lb$. Donc $a|lb$, mais $\text{pgcd}(a, b) = 1$ et d'après le lemme de Gauss $a|l$ donc $l = am$. Par conséquent $c = lb = amb$ et ainsi $ab|c$.

Exemples.

— *Exemple 1.* $273 = 7 \times 39 = 13 \times 21$; donc $13|(7 \times 39)$.
Or $\text{pgcd}(13, 7) = 1$, donc d'après le lemme de Gauss $13|39$.

— *Exemple 2.* Montrons que pour tout $n \in \mathbb{Z}$, $\frac{n(n+1)(n+2)}{6}$ est un entier.
  - Il s'agit de montrer $6|n(n + 1)(n + 2)$. Puisque n et $n + 1$ sont deux entiers consécutifs, l'un des deux est un multiple de 2, donc $2|n(n + 1)$ et a fortiori $2|n(n + 1)(n + 2)$.
  - Pour la même raison, n, $n + 1$ et $n + 2$ sont trois entiers consécutifs donc l'un des trois est un multiple de 3. Ainsi $3|n(n + 1)(n + 2)$.
  - Puisque 2 et 3 sont premiers entre eux, d'après le (corollaire du) lemme de Gauss, 2×3 divise $n(n + 1)(n + 2)$, donc $6|n(n + 1)(n + 2)$.

— *Exemple 3.* Pour finir, remarquons que $6|12$ et $4|12$, mais pourtant $6 \times 4 = 24$ ne divise pas 12 ! Cela vient bien sûr du fait que 6 et 4 ne sont pas premiers entre eux.

— *Exercice.* Montrer que pour tout entier $n \in \mathbb{Z}$, $(n^3 - 4n)(n^2 - 1)$ est un multiple de 15 (et même en fait un multiple de 30).

Autre application du théorème de Bézout

- **Proposition.** Soient deux entiers a et b et $d = \text{pgcd}(a, b)$. Si l'on note $a = da'$ et $b = db'$, alors les entiers a' et b' sont premiers entre eux.
- *Démonstration.* Il s'agit d'une application de la propriété $\text{pgcd}(na, na) = |n| \, \text{pgcd}(a, b)$. En effet, $\text{pgcd}(a, b) = d = \text{pgcd}(da', db') = d \, \text{pgcd}(a', b')$ donc $\text{pgcd}(a', b') = \frac{d}{d} = 1$.
- *Exemple.* Puisque $\text{pgcd}(1\,188, 120) = 12$, alors 12 divise 1 188 et 120. On obtient :

$$\text{pgcd}\left(\frac{1\,188}{12}, \frac{120}{12}\right) = \text{pgcd}(99, 10) = 1$$

  De même, puisque $\text{pgcd}(144, 48) = 48$, on a : $\text{pgcd}(\frac{144}{48}, \frac{48}{48}) = \text{pgcd}(3, 1) = 1$.