PGCD, Bézout et Gauss

Terminale maths expertes · Chapitre 05

Les repères essentiels

- Euclide : $\gcd(a,b) = \gcd(b,r)$; le dernier reste non nul est le PGCD.
- Bézout : $au + bv = d$; une combinaison égale à 1 caractérise les entiers premiers entre eux.
- Gauss : $a \mid bc$ et $\gcd(a,b) = 1$ impliquent $a \mid c$.
- a est inversible modulo n exactement si $\gcd(a,n) = 1$.
- $ax + by = c$ est soluble exactement si $d \mid c$; les solutions s'obtiennent par un paramètre entier.
- Pour $ax \equiv b \pmod{n}$, divise les trois termes par le PGCD lorsque celui-ci divise b.

Contrôle. Ai-je vérifié une identité de Bézout ? La coprimalité exigée par Gauss est-elle établie ? Mon paramètre est-il entier ? Ai-je imposé les éventuelles contraintes de positivité à la fin ?

Une méthode à retenir

> **Méthode · Calculer jusqu'au reste nul**
>
> Remplace d'abord a, b par leurs valeurs absolues. Divise le plus grand par le plus petit, puis le diviseur par le reste. Continue jusqu'au premier reste nul. Le dernier reste non nul est le PGCD.

Un exemple pour se repérer

> **Exemple · Lister sur un petit cas**
>
> Les paires $1 \times 18, 2 \times 9, 3 \times 6$ donnent les diviseurs positifs de 18 : $1, 2, 3, 6, 9, 18$. Pour 30, les paires $1 \times 30, 2 \times 15, 3 \times 10, 5 \times 6$ donnent $1, 2, 3, 5, 6, 10, 15, 30$. En comparant, les nombres présents dans les deux listes sont $1, 2, 3, 6$. Le plus grand est 6 : le PGCD vaut 6. Cela ne signifie pas que 6 est leur seul diviseur commun ; c'est le plus grand diviseur *positif* commun. Les signes négatifs n'ajoutent pas de diviseur positif nouveau.

Les erreurs à éviter

> **Attention · Une contrainte supplémentaire change la réponse**
>
> Les coefficients d'une identité de Bézout peuvent être négatifs. Dans un problème de quantités physiques, on imposera ensuite $x, y \geq 0$. Il faut d'abord résoudre dans les entiers, puis sélectionner les paramètres compatibles avec la situation.