Théorèmes de Bézout et de Gauss

Fiche méthode

(Maths expertes Terminale · Arithmétique)

La démarche pour une question de Bézout ou de Gauss

1. J'identifie l'outil : un PGCD écrit $au + bv$ (identité de Bézout), « premiers entre eux » (théorème de Bézout), une divisibilité à simplifier (Gauss), une équation $ax + by = c$, un inverse modulo n.

2. Je calcule avec l'algorithme d'Euclide, en isolant les restes, puis je remonte.

3. Je cite le théorème avec ses hypothèses vérifiées : « $\text{pgcd}(a\,;b) = 1$ » avant Gauss, « d divise c » avant de résoudre.

4. Je vérifie chaque relation par un calcul direct, et je conclus par un ensemble de solutions avec « $k \in \mathbb{Z}$ » ou par une classe modulo n.

Le réflexe — aucune relation de Bézout sans vérification numérique, aucun « d'après Gauss » sans « premiers entre eux » justifié juste avant.

Cas 1 · Trouver un couple de Bézout

Réflexe — Euclide en isolant les restes, puis remontée depuis le dernier reste non nul, sans effectuer les produits.

Exemple. Questions types : « Déterminer un couple $(u\,;v)$ tel que $au + bv = \text{pgcd}(a\,;b)$ ». Exemple : $67u + 24v = 1$.

$67 = 2 \times 24 + 19$; $24 = 19 + 5$; $19 = 3 \times 5 + 4$; $5 = 4 + 1$.

$1 = 5 - 4 = 4 \times 5 - 19 = 4 \times 24 - 5 \times 19 = 14 \times 24 - 5 \times 67$.

Vérification : $336 - 335 = 1$. Le couple $(-5\,;14)$ convient.

Attention — il y a une infinité de couples : on ne dit pas « le » couple, et on vérifie toujours le sien.

Cas 2 · Prouver que deux entiers sont premiers entre eux

Réflexe — je cherche une combinaison à coefficients entiers égale à 1 ou -1 (en croisant les coefficients de n), puis je cite le théorème de Bézout.

Exemple. Questions types : « Montrer que pour tout entier n, A et B sont premiers entre eux ». Exemple : $4n + 3$ et $5n + 4$.

$5(4n + 3) - 4(5n + 4) = 15 - 16 = -1$.

Donc $(-5)(4n + 3) + 4(5n + 4) = 1$, avec -5 et 4 entiers.

D'après le théorème de Bézout, $4n + 3$ et $5n + 4$ sont premiers entre eux pour tout n.

Attention — une combinaison égale à m $\neq \pm 1$ prouve seulement que le PGCD divise m.

Cas 3 · Simplifier une divisibilité avec Gauss

Réflexe — j'écris « a divise bc » et « pgcd(a ; b) = 1 » avec sa justification, puis je conclus « a divise c ».

Exemple. Questions types : « On suppose que a divise bn. Montrer que a divise n », « Montrer que N est divisible par ab ». Exemple : 15 divise $14n$.

$15 \times 1 - 14 \times 1 = 1$: 15 et 14 sont premiers entre eux (Bézout).

15 divise $14n$ et $\text{pgcd}(15\,;14) = 1$: d'après le théorème de Gauss, 15 divise n.

Attention — si le PGCD n'est pas 1, on divise d'abord par ce PGCD ; et 8 divise 4×6 sans diviser 4 ni 6.

Cas 4 · Résoudre ax + by = c dans $\mathbb{Z}^2$

Réflexe — PGCD, test « d divise c », division par d, solution particulière par Bézout, soustraction et Gauss, réciproque.

Exemple. Questions types : « Résoudre dans $\mathbb{Z}^2$ l'équation … », « Déterminer les solutions telles que … ». Exemple : $11x + 8y = 5$.

$\text{pgcd}(11\,;8) = 1$ et $1 = 3 \times 11 - 4 \times 8$; par 5 : $11 \times 15 + 8 \times (-20) = 5$.
$11(x - 15) = 8(-20 - y)$; 8 divise $11(x - 15)$ et $\text{pgcd}(8\,;11) = 1$, donc $x = 15 + 8k$, puis $y = -20 - 11k$.
$S = \{(15 + 8k\,; -20 - 11k),\ k \in \mathbb{Z}\}$.

Attention — le pas est b ÷ d et a ÷ d, pas b et a ; sans « d divise c », aucune solution.

Cas 5 · Inverse modulo n et équation ax ≡ b [n]

Réflexe — Euclide jusqu'à au + nv = 1, inverse u ramené entre 0 et n − 1, puis x ≡ ub [n].

Exemple. Questions types : « Justifier que a est inversible modulo n et déterminer son inverse », « Résoudre $ax \equiv b\ [n]$ ». Exemple : $13x \equiv 6\ [40]$.

$40 = 3 \times 13 + 1$, donc $13 \times (-3) + 40 = 1$: $\text{pgcd}(13\,;40) = 1$ et l'inverse de 13 est $-3 \equiv 37\ [40]$.
$x \equiv 37 \times 6 = 222 \equiv 22\ [40]$.
Vérification : $13 \times 22 = 286 = 7 \times 40 + 6$.

Attention — l'inverse n'est pas l'opposé ; si pgcd(a ; n) ne divise pas b, il n'y a aucune solution.

Les pièges

- « au + bv = 6, donc pgcd(a ; b) = 6 » : faux, le PGCD divise seulement 6.
- Gauss sans « premiers entre eux » : 4 divise 2 × 6 sans diviser 2 ni 6.
- Corollaire sans « premiers entre eux » : 6 et 9 divisent 18, mais 54 ne divise pas 18.
- Équation ax + by = c : le pas est b ÷ d et a ÷ d (pas b et a), et la réciproque se vérifie.
- Remontée d'Euclide : on garde a et b visibles, on ne calcule pas les produits.
- Une solution d'équation de congruence est une classe modulo n, pas un seul entier.

Ce document est la propriété intellectuelle de Ben, professeur particulier (benprofparticulier.fr), protégée par le Code de la propriété intellectuelle (art. L. 111-1 et L. 122-4). Il est mis à disposition pour un usage personnel de révision. Toute reproduction, diffusion, mise en ligne ou revente, totale ou partielle, sans autorisation écrite est interdite et constitue une contrefaçon (art. L. 335-2).