



Arithmétique dans $\mathbb{Z}$ — Fiche de révision

1ère Bac · Arithmétique dans $\mathbb{Z}$

L'essentiel en une page

Division euclidienne : pour $b > 0$, il existe un unique couple $(q; r)$ tel que $a = bq + r$ avec $0 \leq r < b$.

Notion	Énoncé
Euclide	le PGCD est le dernier reste non nul
Bézout	$\text{PGCD}(a; b) = d \iff \exists u, v, au + bv = d$
Premiers entre eux	$\text{PGCD}(a; b) = 1 \iff \exists u, v, au + bv = 1$
Gauss	$a \mid bc$ et $\text{PGCD}(a; b) = 1 \Rightarrow a \mid c$
Relation	$\text{PGCD} \times \text{PPCM} = ab $

Congruences : $a \equiv b \pmod{n}$ si $n \mid (a - b)$. On peut additionner, multiplier et élever à une puissance les congruences.

Équation $ax + by = c$: elle a des solutions si et seulement si $\text{PGCD}(a; b) \mid c$; on trouve une solution particulière, puis la forme générale $x = x_0 + \frac{b}{d}k$, $y = y_0 - \frac{a}{d}k$.

Puissances modulo n : chercher un exposant p tel que $a^p \equiv 1$, puis réduire l'exposant modulo p .

Ce que je dois savoir faire

- Appliquer l'algorithme d'Euclide et remonter pour obtenir Bézout.
- Résoudre une congruence linéaire en cherchant un inverse.
- Calculer un reste de puissance par réduction cyclique.
- Résoudre une équation diophantienne et donner toutes les solutions.
- Démontrer une divisibilité avec Gauss ou une disjonction des cas.

Les pièges à éviter

- On ne peut pas « diviser » une congruence par un entier quelconque : il faut un **inverse**.
- Gauss exige l'hypothèse « premiers entre eux ».
- Une équation diophantienne a une **infinité** de solutions : ne pas s'arrêter à la particulière.
- Dans $a \equiv b \pmod{n}$, le reste doit être pris entre 0 et $n - 1$.

Testez-vous en 3 minutes

PGCD de 48 et 36 ? Bézout associé ? Reste de 2^{10} modulo 3 ? Solutions de $x \equiv 2 \pmod{5}$?

Réponses

12 ; par exemple $48 - 36 = 12$; $2^{10} = 1\,024 \equiv 1$; $x = 2 + 5k$.