

1ÈRE BAC SCIENCES MATHÉMATIQUES · LEÇON 11

Arithmétique dans $\mathbb{Z}$

Bézout · Gauss · Congruences

Ce que nous allons apprendre

- Division euclidienne et divisibilité
- PGCD et algorithme d'Euclide
- L'identité de Bézout
- Le théorème de Gauss
- Les congruences
- Les équations diophantiennes

Le point de départ

THÉORÈME

Pour $a \in \mathbb{Z}$ et $b > 0$, il existe un **unique** couple $(q; r)$ tel que

$$a = bq + r \quad \text{avec} \quad 0 \leq r < b$$

DIVISIBILITÉ

$b \mid a$ si et seulement si le reste est **nul**.

Calculer un PGCD

Exemple. PGCD de 1 071 et 462.

- ➊ $1\,071 = 2 \times 462 + 147.$
- ➋ $462 = 3 \times 147 + 21.$
- ➌ $147 = 7 \times 21 + 0$: le PGCD est 21.

Remonter l'algorithme

IDENTITÉ DE BÉZOUT

Si $d = \text{PGCD}(a; b)$, il existe des entiers u et v tels que $au + bv = d$.

Suite de l'exemple.

- ❶ $21 = 462 - 3 \times 147.$
- ❷ Or $147 = 1\,071 - 2 \times 462.$
- ❸ Donc $21 = 7 \times 462 - 3 \times 1\,071.$

Un théorème décisif

THÉORÈME DE GAUSS

Si $a \mid bc$ et si $\text{PGCD}(a; b) = 1$, alors $a \mid c$.

- 1 Bézout : il existe u, v tels que $au + bv = 1$.
- 2 En multipliant par c : $acu + bcv = c$.
- 3 a divise les deux termes de gauche, donc $a \mid c$.

Calculer modulo n

DÉFINITION

$a \equiv b \pmod{n}$ si $n \mid (a - b)$.

OPÉRATIONS

On peut **additionner**, **multiplier** et **élever à une puissance** des congruences. On ne peut pas diviser librement.

Exemple. $2^3 = 8 \equiv 1 \pmod{7}$, donc $2^{100} = (2^3)^{33} \times 2 \equiv 2 \pmod{7}$.

Résoudre $ax \equiv b$

Exemple. Résoudre $5x \equiv 3 \pmod{7}$.

- ➊ Je cherche l'inverse de 5 : $5 \times 3 = 15 \equiv 1 \pmod{7}$.
- ➋ Je multiplie par 3 : $x \equiv 9 \equiv 2 \pmod{7}$.
- ➌ $x = 2 + 7k, k \in \mathbb{Z}$.

6 · DIOPHANTIENNES

$$ax + by = c$$

CONDITION D'EXISTENCE

L'équation a des solutions si et seulement si $\text{PGCD}(a; b)$ divise c .

Exemple. $7x + 5y = 1$.

- ➊ Solution particulière : $(3; -4)$ car $21 - 20 = 1$.
- ➋ Solution générale : $x = 3 + 5k, y = -4 - 7k$.

Puissances et chiffre des unités

Énoncé. Chiffre des unités de $3^{2\,024}$?

- 1 Les unités de 3^n suivent le cycle 3, 9, 7, 1 : période 4.
- 2 $2\,024 = 4 \times 506$: on est en fin de cycle.
- 3 Le chiffre des unités est 1.

APPLICATION 1

Divisibilité par 6

Énoncé. Montrer que $n(n + 1)(n + 2)$ est divisible par 6.

- 1 Parmi trois entiers consécutifs, au moins un est pair.
- 2 Exactement un est multiple de 3.
- 3 2 et 3 sont premiers entre eux, donc le produit est divisible par 6.

APPLICATION 2

Un reste rapide

Énoncé. Reste de $5^{2\,023}$ modulo 6 ?

- ➊ $5 \equiv -1 \pmod{6}$.
- ➋ $5^{2\,023} \equiv (-1)^{2\,023} = -1 \pmod{6}$.
- ➌ $-1 \equiv 5$: le reste est 5.

L'essentiel de la leçon

Outil	Énoncé
Euclide	dernier reste non nul
Bézout	$au + bv = d$
Gauss	$a \mid bc$ et $a \wedge b = 1 \Rightarrow a \mid c$
Congruence	somme, produit, puissance
Diophantienne	particulière + générale