

2ÈME BAC SCIENCES MATHÉMATIQUES · LEÇON 10

Arithmétique dans $\mathbb{Z}$

Bézout · Gauss · Congruences · Fermat

Ce que nous allons apprendre

- Division euclidienne et PGCD
- L'algorithme d'Euclide
- Les théorèmes de Bézout et de Gauss
- Congruences modulo n
- Le petit théorème de Fermat
- Équations diophantiennes

Divisibilité et division

DIVISION EUCLIDIENNE

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

PGCD

$\text{PGCD}(a; b) = \text{PGCD}(b; r)$: c'est le cœur de l'algorithme d'Euclide.

Un exemple complet

Exemple. PGCD(2 023 ; 1 071).

- ➊ $2\,023 = 1 \times 1\,071 + 952$.
- ➋ $1\,071 = 1 \times 952 + 119$ puis $952 = 8 \times 119 + 0$.
- ➌ Le dernier reste non nul est 119 : c'est le PGCD.

Remonter l'algorithme

THÉORÈME

Il existe u et v entiers tels que

$$au + bv = \text{PGCD}(a; b)$$

- 1 $119 = 1\,071 - 952.$
- 2 Or $952 = 2\,023 - 1\,071$, d'où $119 = 2 \times 1\,071 - 2\,023.$

Premiers entre eux

RÉCIPROQUE DE BÉZOUT

$au + bv = 1 \Rightarrow a$ et b sont **premiers entre eux**.

THÉORÈME DE GAUSS

Si $a \mid bc$ et $a \wedge b = 1$, alors $a \mid c$.

Calculer modulo n

DÉFINITION

$a \equiv b [n]$ signifie que n divise $a - b$.

OPÉRATIONS

On peut **additionner**, **multiplier** et **élever à une puissance** ; pour « diviser », il faut un **inverse** modulo n .

Réduire une grande puissance

PETIT THÉORÈME DE FERMAT

Si p est **premier** et $p \nmid a$:

$$a^{p-1} \equiv 1 [p]$$

Exemple. $7^{10} \equiv 1 [11]$, donc $7^{100} = (7^{10})^{10} \equiv 1 [11]$.

Reste de $3^{2\,024}$ modulo 7

- 1 7 est premier et $7 \nmid 3 : 3^6 \equiv 1 [7]$.
- 2 $2\,024 = 6 \times 337 + 2$.
- 3 $3^{2\,024} \equiv 3^2 = 9 \equiv 2 [7]$: le reste est 2.

6 · DIOPHANTIENNES

$$\underline{ax + by = c}$$

EXISTENCE

L'équation a des solutions si et seulement si $d = a \wedge b$ **divise** c .

FORME DES SOLUTIONS

$$x = x_0 + \frac{b}{d}k, \quad y = y_0 - \frac{a}{d}k, \quad k \in \mathbb{Z}$$

APPLICATION 1

$$5x - 3y = 1$$

- ❶ $5 \wedge 3 = 1$ divise 1 : il y a des solutions.
- ❷ Solution particulière : $(2; 3)$ car $10 - 9 = 1$.
- ❸ Solutions : $x = 2 + 3k$ et $y = 3 + 5k$, $k \in \mathbb{Z}$.

APPLICATION 2

Un système de congruences

Énoncé. $x \equiv 2 [3]$ et $x \equiv 3 [5]$.

- 1 $x = 2 + 3k$; il faut $2 + 3k \equiv 3 [5]$, soit $3k \equiv 1 [5]$.
- 2 L'inverse de 3 modulo 5 est 2 : $k \equiv 2 [5]$.
- 3 Donc $x = 8 + 15m$, $m \in \mathbb{Z}$.

L'essentiel de la leçon

Théorème	Énoncé
Euclide	dernier reste non nul
Bézout	$au + bv = d$
Gauss	$a \mid bc, a \wedge b = 1 \Rightarrow a \mid c$
Fermat	$a^{p-1} \equiv 1 [p]$
Diophantienne	$d \mid c$