

Chapitre 01 – Cours

Arithmétique des entiers et congruences

Dans ce chapitre, tu vas apprendre à :

- Appliquer Euclide et Bézout
- Résoudre une équation diophantienne
- Raisonner modulo un entier

1. Divisibilité et division euclidienne

Pour des entiers a et b , $a \mid b$ signifie qu'il existe un entier k avec $b = ak$.

Cette relation est compatible avec les combinaisons linéaires : tout diviseur commun de a et b divise $ua + vb$ pour u, v entiers.

Pour un diviseur strictement positif d , chaque entier a s'écrit de manière unique $a = dq + r$, avec $0 \leq r < d$.

Les conditions sur le reste distinguent la division euclidienne d'une simple écriture algébrique.

2. PGCD et algorithme d'Euclide

Le PGCD de deux entiers non tous deux nuls est leur plus grand diviseur commun positif.

L'identité $\gcd(a, b) = \gcd(b, a - qb)$ explique l'algorithme d'Euclide : remplacer successivement un couple par le diviseur et le reste.

Les restes positifs diminuent strictement, donc la procédure termine.

Le dernier reste non nul est le PGCD.

On peut remonter les divisions pour écrire ce PGCD comme combinaison linéaire des deux nombres initiaux.

3. Bézout et Gauss

Deux entiers sont premiers entre eux si et seulement s'il existe u, v entiers tels que $ua + vb = 1$.

Le sens direct repose sur l'algorithme d'Euclide ; le sens réciproque est immédiat puisqu'un diviseur commun divise alors 1.

Le lemme de Gauss affirme que si a divise bc et est premier avec b , alors a divise c .

Cette hypothèse de coprimauté est essentielle : $6 \mid 2 \times 3$ mais 6 ne divise ni 2 ni 3.

4. Équations diophantiennes

Pour a, b non tous deux nuls, l'équation $ax + by = c$ admet des solutions entières si et seulement si $\gcd(a, b)$ divise c .

Une identité de Bézout fournit une solution particulière lorsque cette condition est satisfaite.

Pour obtenir toutes les solutions, on soustrait cette solution et on applique Gauss après division par le PGCD.

Il faut distinguer une solution trouvée par essai et la description de l'ensemble complet des couples entiers.

5. Congruences et nombres premiers

La congruence $a \equiv b \pmod{m}$ signifie que m divise $a - b$.

Elle respecte sommes et produits, donc puissances entières positives.

On ne peut simplifier un facteur arbitrairement : une classe a possède un inverse modulo m exactement lorsque $\gcd(a, m) = 1$.

Bézout donne cet inverse.

Pour un nombre premier p , tout entier non divisible par p possède un inverse modulo p ; le petit théorème de Fermat donne $a^{p-1} \equiv 1 \pmod{p}$ pour un tel a .

6. Méthode et contrôle

Une décomposition en facteurs premiers permet de calculer PGCD et PPCM par les exposants minimaux et maximaux.

Une preuve de primalité par divisions exige seulement les nombres premiers ne dépassant pas la racine carrée du candidat.

Pour une congruence, on annonce le module, on réduit les bases puis on exploite une périodicité démontrée.

Un reste final doit appartenir à $\{0, \dots, m - 1\}$.

L'arithmétique sert ici à comprendre les structures, et non à tester de très grands nombres sans justification.

Les hypothèses rendent la simplification possible

Définition – Inverse modulo un entier

Pour $m \geq 2$, un inverse de a modulo m est un entier u tel que $au \equiv 1 \pmod{m}$. Il existe exactement lorsque a et m sont premiers entre eux. Sa classe modulo m est alors unique, mais ses représentants entiers sont multiples.

Exemple résolu – 1. Remonter Euclide puis résoudre

Résolvons $26x + 15y = 1$ dans $\mathbb{Z}^2$.

1. Effectuer les divisions : $26 = 15 + 11$, $15 = 11 + 4$, $11 = 2 \times 4 + 3$, $4 = 3 + 1$. Le dernier reste non nul vaut 1 ; le PGCD est donc 1.
2. Remonter donne $1 = 4 - 3 = 3 \times 4 - 11 = 3 \times 15 - 4 \times 11 = 7 \times 15 - 4 \times 26$. Une solution particulière est $(x_0, y_0) = (-4, 7)$.
3. Pour toute autre solution, $26(x + 4) = -15(y - 7)$. Gauss impose $x + 4 = 15t$, puis $y - 7 = -26t$, avec $t \in \mathbb{Z}$.

$$\mathcal{S} = \{(-4 + 15t, 7 - 26t) : t \in \mathbb{Z}\}.$$

Réciproquement, la substitution vérifie chaque couple de cette famille.

Exemple résolu – 2. Simplifier une congruence avec précaution

Résolvons $6x \equiv 9 \pmod{15}$.

1. La congruence signifie $6x - 9 = 15k$ pour un entier k . Les trois termes sont divisibles par 3, d'où $2x - 3 = 5k$.
2. L'équation équivaut donc à $2x \equiv 3 \pmod{5}$. L'inverse de 2 modulo 5 est 3, car $2 \times 3 \equiv 1 \pmod{5}$.
3. Multiplier par 3 donne $x \equiv 9 \equiv 4 \pmod{5}$. Modulo 15, cela correspond aux trois classes 4, 9, 14.

Diviser par le diviseur commun a changé le module de 15 en 5. Conserver 15 après cette division ferait perdre des solutions.

Les divisions réduisent le problème

$$\begin{array}{c}
 \boxed{(26, 15)} \\
 \downarrow \\
 \boxed{(15, 11)} \\
 \downarrow \\
 \boxed{(11, 4)} \\
 \downarrow \\
 \boxed{(4, 3)} \\
 \downarrow \\
 \boxed{(3, 1)}
 \end{array}
 \begin{array}{l}
 26 = 1 \times 15 + 11 \\
 15 = 1 \times 11 + 4 \\
 11 = 2 \times 4 + 3 \\
 4 = 1 \times 3 + 1
 \end{array}$$

Chaque flèche conserve les diviseurs communs et diminue strictement le second entier positif. Le schéma s'arrête au reste 1 ; la division suivante serait $3 = 3 \times 1 + 0$. Remonter les flèches reconstruit une identité de Bézout.

À retenir – Bilan

Divisibilité et congruence portent sur des entiers et un module précisé. Euclide calcule le PGCD ; sa remontée fournit Bézout ; Gauss décrit toutes les solutions après réduction par le PGCD. Une simplification modulo m exige un facteur inversible ou un ajustement justifié du module.
