DIVISIBILITÉ ET CONGRUENCES

COURS

Divisibilité et congruences

DURÉE ESTIMÉE

20 minutes

OBJECTIFS DU CHAPITRE

- Calculer un reste à l'aide de congruences
- Effectuer une division euclidienne dans Z
- Démontrer une divisibilité à l'aide de combinaisons linéaires
- Démontrer une divisibilité par disjonction des cas modulo n
- Démontrer une propriété de divisibilité par récurrence
- Résoudre une congruence linéaire ax = b [n]

1. Divisibilité dans $\mathbb{Z}$

Définition

Soient a et b deux entiers relatifs. On dit que b **divise** a s'il existe un entier relatif k tel que $a = bk$.

On dit alors que :

- b est un **diviseur** de a ;
- a est un **multiple** de b.

Cela se note $b \mid a$.

Exemple

$15 = 3 \times 5$ donc 3 divise 15 : 3 est un diviseur de 15 et 15 est un multiple de 3.

Remarque

- 0 est un multiple de tout entier relatif.
- 1 et -1 sont des diviseurs de tout entier relatif.
- a et $-a$ ont les mêmes diviseurs.

Propriétés de la divisibilité

Soient a, b et c trois entiers relatifs.

- Si a divise b et b divise a, alors a et b sont égaux ou opposés.
- Si a divise b et b divise c, alors a divise c (transitivité).
- Si c divise a et c divise b, alors c divise toute combinaison linéaire de a et b, c'est-à-dire tout nombre de la forme $au + bv$ avec $u \in \mathbb{Z}$ et $v \in \mathbb{Z}$.

Exemple

7 divise 21 et 7 divise 35. Donc 7 divise $3 \times 21 - 2 \times 35 = 63 - 70 = -7$, ce qui est bien le cas.

2. Division euclidienne dans $\mathbb{Z}$

Division euclidienne dans $\mathbb{Z}$

Soient a et b deux entiers relatifs avec $b \neq 0$.

Il existe un unique couple d'entiers relatifs (q, r) tel que :

$$a = bq + r \quad \text{et} \quad 0 \leqslant r < |b|$$

q s'appelle le **quotient** et r le **reste** de la **division euclidienne** de a par b.

Exemple

$-14 = 3 \times (-5) + 1$ et $0 \leqslant 1 < 3$.

La division euclidienne de -14 par 3 donne donc un quotient égal à -5 et un reste égal à 1.

Remarque

- **Attention !** La condition $0 \leqslant r < |b|$ est essentielle. La seule égalité $a = bq + r$ ne suffit pas à prouver que q et r sont les quotient et reste de la division euclidienne de a par b.

- a est divisible par b si et seulement si le reste de la division euclidienne de a par b est égal à zéro.

3. Congruences modulo n

Définition

Soit n un entier naturel non nul. On dit que deux entiers relatifs a et b sont **congrus modulo** n et l'on écrit

$$a \equiv b \ [n]$$

si et seulement si a et b ont le même reste dans la division euclidienne par n.

Exemple

$18 \equiv 23 \ [5]$ car 18 et 23 ont tous les deux 3 comme reste dans la division euclidienne par 5.

Caractérisation par la divisibilité

- $a \equiv b \ [n]$ si et seulement si n divise $a - b$.
- En particulier, $a \equiv 0 \ [n]$ si et seulement si n divise a.
- Si $a \equiv b \ [n]$ et $b \equiv c \ [n]$, alors $a \equiv c \ [n]$ (transitivité).

Congruences et opérations

Soient quatre entiers relatifs a, b, c, d tels que $a \equiv b \ [n]$ et $c \equiv d \ [n]$. Alors :

- $a + c \equiv b + d \ [n]$ et $a - c \equiv b - d \ [n]$;
- $ac \equiv bd \ [n]$;
- $ka \equiv kb \ [n]$ pour tout entier relatif k ;
- $a^m \equiv b^m \ [n]$ pour tout entier naturel m.

Caractérisation du reste par les congruences

r est le reste de la division euclidienne de a par b (avec $b > 0$) si et seulement si :

$$\begin{cases} a \equiv r \ [b] \\ 0 \leqslant r < b \end{cases}$$

Exemple

On cherche le reste de la division euclidienne de 2009^{2009} par 5.

$2009 \equiv -1 \ [5]$ car $2009 - (-1) = 2010$ est divisible par 5.

Donc $2009^{2009} \equiv (-1)^{2009} \ [5]$, c'est-à-dire $2009^{2009} \equiv -1 \ [5]$.

Or $-1 \equiv 4 \ [5]$ donc $2009^{2009} \equiv 4 \ [5]$.

Comme $0 \leqslant 4 < 5$, le reste de la division euclidienne de 2009^{2009} par 5 est 4.

Les questions essentielles

1. Comment effectuer une division euclidienne dans $\mathbb{Z}$ quand le dividende est négatif ?

On part de la division usuelle de la valeur absolue, puis on ajuste le quotient et le reste pour que la condition $0 \leqslant r < |b|$ soit respectée.

Voir la fiche méthode : Effectuer une division euclidienne dans Z

2. Comment démontrer qu'un entier en divise un autre ?

On exprime le nombre cible comme une combinaison linéaire de deux multiples connus du diviseur, en s'appuyant sur la propriété : si $c \mid a$ et $c \mid b$, alors $c \mid au + bv$.

Voir la fiche méthode : Démontrer une divisibilité à l'aide de combinaisons linéaires

3. Comment démontrer qu'une expression est divisible par un entier p pour tout entier n ?

On raisonne par disjonction selon les p valeurs possibles de n modulo p et on vérifie que l'expression est bien congrue à 0 dans

chaque cas.

Voir la fiche méthode : Démontrer une divisibilité par disjonction des cas modulo n

4. Comment démontrer une divisibilité contenant une puissance a^n ?

Lorsque l'expression contient une puissance ou une factorielle, on rédige une **démonstration par récurrence** : initialisation au premier rang, hérédité en substituant l'hypothèse de récurrence dans le terme dominant.

Voir la fiche méthode : Démontrer une propriété de divisibilité par récurrence

5. Comment trouver le reste de la division d'une grande puissance par les congruences ?

On cherche un représentant simple (± 1, ± 2...) de la base modulo n, puis on élève à la puissance demandée et on ramène le résultat dans $[0, n[$.

Voir la fiche méthode : Calculer un reste à l'aide de congruences

6. Comment résoudre une congruence linéaire $ax \equiv b\ [n]$?

On teste les valeurs de x parmi les restes possibles modulo n, ou l'on simplifie la congruence à l'aide d'un inverse de a modulo n lorsqu'il existe.

Voir la fiche méthode : Résoudre une congruence linéaire ax = b [n]

Télécharger en PDF