Arithmétique

1ère Année Baccalauréat – Sciences Mathématiques

Volume horaire officiel : 13h (cf. répartition 2013) – **Pré-requis** : raisonnement par récurrence, ensembles, suites.
Capacités attendues : utiliser l'algorithme d'Euclide pour déterminer le PGCD de deux entiers ; reconnaître les règles de calcul sur les congruences ; utiliser les congruences pour étudier la divisibilité et inversement.

Table des matières

1. Divisibilité dans $\mathbb{Z}$

1.1 Définition

Définition

Définition 1.1 — Soient $a, b \in \mathbb{Z}$. On dit que a **divise** b (ou b est **multiple** de a), et on note $a \mid b$, s'il existe $k \in \mathbb{Z}$ tel que $b = ka$.

Exemples : $3 \mid 12$ ($12 = 4 \cdot 3$), $-5 \mid 20$, $0 \mid 0$, $1 \mid n$ pour tout n.

1.2 Propriétés

Propriété

Propriété 1.1 — Pour tous $a, b, c \in \mathbb{Z}$:

(a) Réflexivité : $a \mid a$.
(b) Transitivité : $a \mid b$ et $b \mid c \Rightarrow a \mid c$.
(c) Antisymétrie : $a \mid b$ et $b \mid a \Rightarrow a = \pm b$.
(d) Linéarité : si $a \mid b$ et $a \mid c$, alors $a \mid (\alpha b + \beta c)$ pour tous $\alpha, \beta \in \mathbb{Z}$.
(e) $a \mid b$ et $b \neq 0 \Rightarrow |a| \leq |b|$.
(f) $a \mid b \Rightarrow a \mid b^n$ pour tout $n \in \mathbb{N}^*$.

Démonstration

(d) Linéarité. Si $b = ak_1$ et $c = ak_2$, alors $\alpha b + \beta c = a(\alpha k_1 + \beta k_2)$, qui est multiple de a. □

2. Division euclidienne

Théorème

Théorème 2.1 — **(Division euclidienne)** Pour tous $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$, il existe un *unique* couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que :

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

q est le **quotient** et r le **reste** de la division euclidienne de a par b.

Remarque

a est divisible par b ssi $r = 0$.

Exemple

Exemple 2.1 — Division euclidienne de 73 par 11 : $73 = 11 \cdot 6 + 7$, donc $q = 6$, $r = 7$.
Division euclidienne de -73 par 11 : $-73 = 11 \cdot (-7) + 4$, donc $q = -7$, $r = 4$ (et non -6 et -7).

3. PGCD et algorithme d'Euclide

3.1 PGCD

Définition

Définition 3.1 — Soient $a, b \in \mathbb{Z}$ non tous deux nuls. Le **plus grand commun diviseur** de a et b, noté $\text{pgcd}(a, b)$ ou $a \wedge b$, est le plus grand entier strictement positif qui divise à la fois a et b.
Par convention, $\text{pgcd}(0, 0)$ n'est pas défini ; $\text{pgcd}(a, 0) = |a|$ pour $a \neq 0$.

Propriété

Propriété 3.1 —

$$\text{pgcd}(a, b) = \text{pgcd}(b, a) \quad ; \quad \text{pgcd}(a, b) = \text{pgcd}(|a|, |b|).$$

3.2 Algorithme d'Euclide

Théorème

Théorème 3.1 — **(Lemme d'Euclide)** Pour $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$, si $a = bq + r$ (avec $0 \leq r < b$), alors :

$$\text{pgcd}(a, b) = \text{pgcd}(b, r).$$

Démonstration

Tout diviseur commun de a et b divise $r = a - bq$ (linéarité), donc est diviseur commun de b et r. Inversement, tout diviseur commun de b et r divise $a = bq + r$, donc est diviseur commun de a et b. Les ensembles de diviseurs communs coïncident, leurs plus grands éléments aussi. □

Méthode

Algorithme d'Euclide pour calculer $\text{pgcd}(a, b)$ **:**

1. Effectuer la division euclidienne : $a = bq_1 + r_1$ avec $0 \leq r_1 < b$.
2. Si $r_1 = 0$, pgcd $= b$.
3. Sinon, $\text{pgcd}(a, b) = \text{pgcd}(b, r_1)$: on recommence avec b et r_1.

La suite des restes est strictement décroissante et finit toujours par atteindre 0. Le *dernier reste non nul* est le PGCD.

Exemple

Exemple 3.1 — Calculer $\text{pgcd}(252, 198)$.

Solution.

$$\begin{aligned} 252 &= 198 \cdot 1 + 54 \\ 198 &= 54 \cdot 3 + 36 \\ 54 &= 36 \cdot 1 + 18 \\ 36 &= 18 \cdot 2 + 0. \end{aligned}$$

Dernier reste non nul : $\text{pgcd}(252, 198) = 18$.

3.3 Identité de Bézout

Théorème

Théorème 3.2 — **(Bézout)** Pour $a, b \in \mathbb{Z}$ non tous deux nuls, il existe $u, v \in \mathbb{Z}$ tels que :

$$au + bv = \text{pgcd}(a, b).$$

On les trouve par l'**algorithme d'Euclide étendu** (on remonte les calculs).

Exemple

Exemple 3.2 — Trouver u, v tels que $252u + 198v = 18$.

Solution. En reprenant l'exemple précédent :

$$\begin{aligned} 18 &= 54 - 36 \cdot 1 \\ &= 54 - (198 - 54 \cdot 3) = 54 \cdot 4 - 198 \\ &= (252 - 198) \cdot 4 - 198 = 252 \cdot 4 - 198 \cdot 5. \end{aligned}$$

Donc $u = 4$, $v = -5$. Vérification : $252 \cdot 4 - 198 \cdot 5 = 1008 - 990 = 18$. ✓

3.4 Nombres premiers entre eux

Définition

Définition 3.2 — On dit que a et b sont **premiers entre eux** si $\text{pgcd}(a, b) = 1$.

Théorème

Théorème 3.3 — **(Théorème de Bézout)** a et b sont premiers entre eux ssi il existe $u, v \in \mathbb{Z}$ tels que $au + bv = 1$.

Théorème

Théorème 3.4 — **(Lemme de Gauss)** Si $a \mid bc$ et $\text{pgcd}(a, b) = 1$, alors $a \mid c$.

Démonstration

Par Bézout, $au + bv = 1$ pour certains u, v. Multiplions par c : $auc + bcv = c$. Comme $a \mid auc$ et $a \mid bc$, on a $a \mid (auc + bcv) = c$. □

3.5 PPCM

Définition

Définition 3.3 — Le **plus petit commun multiple** de $a, b \in \mathbb{Z}^*$, noté $\text{ppcm}(a, b)$ ou $a \vee b$, est le plus petit entier strictement positif qui est multiple à la fois de a et b.

Propriété

Propriété 3.2 — Pour $a, b \in \mathbb{N}^*$:

$$\text{pgcd}(a, b) \cdot \text{ppcm}(a, b) = ab.$$

4. Congruences

4.1 Définition

Définition

Définition 4.1 — Soient $a, b \in \mathbb{Z}$ et $n \in \mathbb{N}^*$. On dit que a est **congru** à b **modulo** n, et on note $a \equiv b \pmod{n}$, si $n \mid (a-b)$.

De manière équivalente : a et b ont le *même reste* dans la division euclidienne par n.

Exemple

Exemple 4.1 — $17 \equiv 5 \pmod{12}$ (car $17-5=12$).
$-7 \equiv 3 \pmod{5}$ (car $-7-3=-10$).
Tout entier est congru à un unique reste modulo n, élément de $\{0, 1, \ldots, n-1\}$.

4.2 Propriétés

Propriété

Propriété 4.1 — **(Relation d'équivalence)** Pour tous $a, b, c \in \mathbb{Z}$ et $n \in \mathbb{N}^*$:

(a) Réflexivité : $a \equiv a \pmod{n}$.
(b) Symétrie : $a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n}$.
(c) Transitivité : $a \equiv b \pmod{n}$ et $b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n}$.

Théorème

Théorème 4.1 — **(Règles de calcul)** Si $a \equiv a' \pmod{n}$ et $b \equiv b' \pmod{n}$, alors :

$$a+b \equiv a'+b' \pmod{n} \quad ; \quad ab \equiv a'b' \pmod{n} \quad ; \quad a^k \equiv (a')^k \pmod{n} \ (k \in \mathbb{N}).$$

Remarque

Attention : la simplification par un diviseur commun n'est pas toujours valide. On peut diviser par c ssi $\text{pgcd}(c, n) = 1$.

Ex : $4 \equiv 10 \pmod{6}$ mais on ne peut pas simplifier par 2 ($\text{pgcd}(2,6) = 2 \neq 1$) : on aurait $2 \equiv 5 \pmod{6}$, ce qui est faux.

4.3 Applications aux congruences

Exemple

Exemple 4.2 — Montrer que pour tout $n \in \mathbb{N}$, $7^n - 1$ est divisible par 6.

Solution avec congruences. $7 \equiv 1 \pmod{6}$, donc $7^n \equiv 1^n = 1 \pmod{6}$, soit $7^n - 1 \equiv 0 \pmod{6}$.

Exemple

Exemple 4.3 — Déterminer le reste de la division de 3^{100} par 7.

Solution. On cherche les puissances de 3 $\pmod{7}$:

$$3^1 = 3,\ 3^2 = 9 \equiv 2,\ 3^3 \equiv 6,\ 3^4 \equiv 18 \equiv 4,\ 3^5 \equiv 12 \equiv 5,\ 3^6 \equiv 15 \equiv 1 \pmod{7}.$$

Cycle de longueur 6. Donc $3^{100} = 3^{6 \cdot 16+4} = (3^6)^{16} \cdot 3^4 \equiv 1 \cdot 4 = 4 \pmod{7}$.

Reste : 4.

4.4 Critères de divisibilité

Propriété

Propriété 4.2 — Soit $n = \overline{a_k a_{k-1} \cdots a_1 a_0}$ l'écriture en base 10 d'un entier.

- n divisible par 2 $\Leftrightarrow$ $a_0 \in \{0, 2, 4, 6, 8\}$.
- n divisible par 5 $\Leftrightarrow$ $a_0 \in \{0, 5\}$.
- n divisible par 3 $\Leftrightarrow$ $a_0 + a_1 + \cdots + a_k$ divisible par 3.
- n divisible par 9 $\Leftrightarrow$ $a_0 + a_1 + \cdots + a_k$ divisible par 9.
- n divisible par 11 $\Leftrightarrow$ $a_0 - a_1 + a_2 - \cdots$ divisible par 11.

5. Synthèse

5.1 Récapitulatif

Notion	Caractérisation
$a \mid b$	$\exists k \in \mathbb{Z},\ b = ka$
Division euclidienne	$a = bq + r,\ 0 \leq r < b$ (unique)
PGCD	plus grand diviseur commun, calculé par Euclide
Bézout	$au + bv = \text{pgcd}(a, b)$ pour certains $u, v \in \mathbb{Z}$
Premiers entre eux	$\text{pgcd}(a, b) = 1 \Leftrightarrow \exists u, v,\ au + bv = 1$
Gauss	$a \mid bc$ et $\text{pgcd}(a, b) = 1 \Rightarrow a \mid c$
PPCM	$\text{ppcm}(a, b) \cdot \text{pgcd}(a, b) = ab$ (pour $a, b > 0$)
Congruence	$a \equiv b \pmod{n} \Leftrightarrow n \mid (a - b)$

5.2 Pièges classiques

Remarque

1. **Division euclidienne avec $a < 0$.** Le reste est toujours ≥ 0.
2. **Simplification dans une congruence.** On ne peut diviser par c que si $\text{pgcd}(c, n) = 1$.
3. $\text{pgcd}(a, 0) = |a|$**.** Cas particulier souvent oublié.
4. **Bézout fonctionne seulement avec le PGCD.** L'équation $au + bv = c$ a des solutions ssi $\text{pgcd}(a, b) \mid c$.
5. **Critère de divisibilité par 11.** Alternance des signes.

Fin du chapitre 4 – Arithmétique