Arithmétique dans $\mathbb{Z}$

الحسابيات في $\mathbb{Z}$

📚 Résumé du cours

I. Divisibilité dans $\mathbb{Z}$

Définition

Soient a, b $\in \mathbb{Z}$ avec b $\neq$ 0. On dit que **b divise a**, noté **b | a**, s'il existe k $\in \mathbb{Z}$ tel que **a = k \cdot b**.

On dit aussi que a est un **multiple** de b, ou que b est un **diviseur** de a.

Propriétés

- 1 | a et a | a pour tout a $\in \mathbb{Z}^*$.
- Si a | b et b | c, alors a | c *(transitivité)*.
- Si a | b et a | c, alors a | (αb + βc) pour tous α, $\beta \in \mathbb{Z}$ *(combinaison linéaire)*.
- Si a | b et b | a (a, b non nuls), alors |a| = |b|, soit a = ±b.
- Si a | b et b $\neq$ 0, alors |a| $\leq$ |b|.

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

Théorème

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 :

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

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

Exemple

Pour a = −17 et b = 5 : −17 = 5·(−4) + 3 avec $0 \leq 3 < 5$. Donc q = −4 et r = 3.

III. Congruences modulo n

Définition

Soit n $\in \mathbb{N}^*$. On dit que a et b sont **congrus modulo n**, noté **a ≡ b [n]**, si n divise (a − b), c'est-à-dire si a et b ont le même reste dans la division euclidienne par n.

Propriétés des congruences

Soient a, b, c, d $\in \mathbb{Z}$ et n $\in \mathbb{N}^*$. Si a ≡ b [n] et c ≡ d [n], alors :

- **a + c ≡ b + d [n]** (somme)
- **a − c ≡ b − d [n]** (différence)
- **a \cdot c ≡ b \cdot d [n]** (produit)
- $a^k \equiv b^k$ **[n]** pour tout k $\in \mathbb{N}$ (puissance)

Attention : on ne peut pas toujours diviser les congruences. a·c ≡ b·c [n] n'implique pas a ≡ b [n].

Applications

- **Reste d'une puissance :** calcul efficace de a^n mod p.
- **Critères de divisibilité :** par 3 (somme des chiffres), par 9, par 11, etc.
- **Équations diophantiennes :** résolution modulo un nombre bien choisi.

IV. PGCD (plus grand commun diviseur)

Définition

Soient a, b ∈ ℤ non tous deux nuls. Le **PGCD** de a et b, noté **pgcd(a, b)** ou **a ∧ b**, est le plus grand entier positif qui divise à la fois a et b.

Algorithme d'Euclide

Si a = bq + r avec $0 \leq r < b$, alors **pgcd(a, b) = pgcd(b, r)**.

On itère jusqu'à obtenir un reste nul : le dernier reste non nul est le pgcd.

Exemple — pgcd(84, 30)

84 = 30·2 + 24 ⇒ pgcd(84, 30) = pgcd(30, 24)
30 = 24·1 + 6 ⇒ pgcd(30, 24) = pgcd(24, 6)
24 = 6·4 + 0 ⇒ pgcd(24, 6) = 6
Donc **pgcd(84, 30) = 6**.

Propriétés

- pgcd(a, b) = pgcd(|a|, |b|)
- pgcd(ka, kb) = |k|·pgcd(a, b) pour k ∈ $\mathbb{Z}^*$
- pgcd(a, 0) = |a|
- pgcd(a, b)·ppcm(a, b) = |a·b|

V. Théorème de Bézout

Identité de Bézout

Pour tous a, b ∈ ℤ non tous deux nuls, il existe u, v ∈ ℤ tels que :

au + bv = pgcd(a, b)

Théorème de Bézout (forme caractéristique)

Deux entiers a et b sont **premiers entre eux** (pgcd(a, b) = 1) **si et seulement si** il existe u, v ∈ ℤ tels que **au + bv = 1**.

Algorithme d'Euclide étendu

Pour déterminer u et v explicitement, on « remonte » les divisions successives.

VI. Théorème de Gauss

Soient a, b, c $\in \mathbb{Z}$. Si **a | bc** et **pgcd(a, b) = 1**, alors **a | c**.

Corollaires

- Si pgcd(a, b) = 1 et a | n, b | n, alors ab | n.
- Si a | c, b | c et pgcd(a, b) = 1, alors ab | c.

VII. PPCM (plus petit commun multiple)

Définition

Le **PPCM** de a et b (non nuls), noté **ppcm(a, b)** ou **a ∨ b**, est le plus petit entier strictement positif multiple à la fois de a et de b.

Relation fondamentale

$$\text{pgcd}(a, b) \times \text{ppcm}(a, b) = |a \times b|$$

VIII. Nombres premiers

Définition

Un entier p ≥ 2 est **premier** s'il n'admet que deux diviseurs positifs : 1 et lui-même.

Exemples : 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, ...

Lemme d'Euclide

Si p est premier et p | ab, alors **p | a ou p | b**.

Théorème fondamental de l'arithmétique

Tout entier n ≥ 2 s'écrit de manière **unique** (à l'ordre près) comme produit de nombres premiers :

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$$

Théorème (Euclide)

L'ensemble des nombres premiers est **infini**.

Test de primalité

Pour vérifier que n est premier, il suffit de vérifier qu'il n'est divisible par aucun nombre premier p ≤ $\sqrt{n}$.

Exemple : pour tester 97, on vérifie les premiers p ≤ $\sqrt{97} \approx 9.8$: 2, 3, 5, 7. Aucun ne divise 97 ⇒ 97 est premier.

IX. Équations diophantiennes ax + by = c

Critère de résolubilité

L'équation **ax + by = c** (a, b, c $\in \mathbb{Z}$, (a, b) ≠ (0, 0)) admet des solutions entières **si et seulement si** pgcd(a, b) | c.

Méthode de résolution

1. Calculer d = pgcd(a, b). Si d ne divise pas c : pas de solution.
2. Sinon, diviser toute l'équation par d pour se ramener à a'x + b'y = c' avec pgcd(a', b') = 1.
3. Trouver une solution particulière (x_0, y_0) par Bézout.
4. Solution générale : **(x, y) = (x_0 + b'k ; y_0 – a'k)** pour k ∈ $\mathbb{Z}$.

🎯 Formules clés

- **Division euclidienne :** a = bq + r avec $0 \leq r < b$ (unique)
- **Congruence :** a ≡ b [n] ⇔ n | (a–b)
- **Opérations :** les congruences respectent +, –, ×, puissance
- **Algorithme d'Euclide :** pgcd(a, b) = pgcd(b, a mod b)
- **Bézout :** pgcd(a, b) = 1 ⇔ ∃ u, v ∈ $\mathbb{Z}$: au + bv = 1
- **Gauss :** a | bc et pgcd(a,b) = 1 ⇒ a | c
- **PGCD × PPCM :** pgcd(a, b) · ppcm(a, b) = |ab|
- **Décomposition unique** en facteurs premiers
- **ax + by = c** a des solutions ⇔ pgcd(a, b) | c

💡 Astuces & méthodes

🔴 Pièges classiques

❌

Congruence et division : a ≡ 0 [n] signifie que n | a. Mais a ≡ b [n] ne signifie PAS a/n = b — ça signifie que a et b ont le même reste dans la division par n.

❌

Théorème de Gauss mal appliqué : pour conclure a | c depuis a | bc, il faut ABSOLUMENT que pgcd(a,b)=1. Si pgcd(a,b) ≠ 1, la conclusion peut être fausse.

❌

Équation diophantienne : trouver la solution générale : après avoir trouvé une solution particulière (x_0 , y_0), la solution générale est (x_0 + b'k, y_0 − a'k) avec k ∈ $\mathbb{Z}$ (après division par pgcd). Ne pas oublier le k !

🟢 Astuces de pros

✅

Congruences pour les derniers chiffres : le dernier chiffre de a^n dépend uniquement de a mod 10. Les puissances de 2 : 2,4,8,6,2,4,8,6... (période 4). Très utile pour les calculs modulaires !

✅

Algorithme d'Euclide étendu pour Bézout : remonte les étapes de l'algorithme d'Euclide pour exprimer pgcd(a,b) comme combinaison linéaire de a et b. Pratique pour trouver une solution particulière.

💡

Preuve de primalité : pour montrer qu'un nombre n est premier, il suffit de vérifier qu'il n'est divisible par aucun nombre premier ≤ $\sqrt{n}$. Si $\sqrt{100}$ = 10, tester seulement 2, 3, 5, 7.