

ARITHMÉTIQUE DANS L'ENSEMBLE $\mathbb{Z}$ 2^{ème} BAC SCIENCES MATHÉMATIQUES1 DIVISIBILITÉ DANS $\mathbb{Z}$

a divise b s'il existe $k \in \mathbb{Z}$ tel que :

$$b = ak$$

On note : $a \mid b$

Exemples :

- $3 \mid 12$
- $5 \nmid 18$

2 DIVISION EUCLIDIENNE

Pour tout $a \in \mathbb{Z}$ et tout $b \in \mathbb{Z}^*$,

il existe des entiers uniques q et r tels que :

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

q : quotient, r : reste

Exemple : $23 = 5 \times 4 + 3$

3 PGCD – PLUS GRAND COMMUN DIVISEUR

Le PGCD de a et b est le plus grand entier positif divisant a et b .

On note : $\gcd(a, b)$

Méthode d'Euclide : divisions successives jusqu'à obtenir un reste nul.

Le dernier reste non nul est le PGCD.

Exemple :

$$45 = 30 \times 1 + 15$$

$$30 = 15 \times 2 + 0$$

Donc : $\gcd(45, 30) = 15$

4 NOMBRES PREMIERS ENTRE EUX

Deux entiers a et b sont premiers entre eux si et seulement si :

$$\gcd(a, b) = 1$$

Exemple : 8 et 15

5 THÉORÈME DE BÉZOUT

Les entiers a et b sont premiers entre eux si et seulement s'il existe $u, v \in \mathbb{Z}$ tels que :

$$au + bv = 1$$

Exemple : $3 \times 5 + (-2) \times 7 = 1$

Donc 5 et 7 sont premiers entre eux.

6 THÉORÈME DE GAUSS

Si $a \mid bc$ et $\gcd(a, b) = 1$

alors $a \mid c$

Très important dans les démonstrations.

7 PPCM – PLUS PETIT COMMUN MULTIPLE

Le PPCM de a et b est le plus petit entier positif multiple de a et de b .

On note : $\text{ppcm}(a, b)$

Relation fondamentale :

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

8 NOMBRES PREMIERS

Définition : Un entier naturel $p \geq 2$ est premier s'il possède exactement deux diviseurs positifs : 1 et p .

Exemples : 2, 3, 5, 7, 11, 13, ...

9 DÉCOMPOSITION EN FACTEURS PREMIERS

Tout entier $n \geq 2$ peut s'écrire sous la forme :

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

où les p_i sont des nombres premiers.

Exemple : $84 = 2^2 \times 3 \times 7$

10 CONGRUENCE MODULO n

a est congru à b modulo n si :

$$a \equiv b \pmod{n}$$

c'est-à-dire $n \mid (a - b)$

Exemple : $17 \equiv 5 \pmod{12}$ car $17 - 5 = 12$

11 PROPRIÉTÉS DES CONGRUENCES

Si $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n}$ alors :

- Addition : $a + c \equiv b + d \pmod{n}$
- Soustraction : $a - c \equiv b - d \pmod{n}$
- Multiplication : $ac \equiv bd \pmod{n}$
- Puissance : $a^p \equiv b^p \pmod{n}$

12 ÉQUATIONS DIOPHANTIENNES

Équation de la forme :

$$ax + by = c \quad (a, b, c \in \mathbb{Z})$$

Condition d'existence :

L'équation admet des solutions entières si et seulement si :

$$\gcd(a, b) \mid c$$

Méthode : utiliser l'algorithme d'Euclide et le théorème de Bézout.

13 RÉSUMÉ DES OUTILS ESSENTIELS

- ✓ Division euclidienne
- ✓ Algorithme d'Euclide (PGCD)
- ✓ Théorème de Bézout
- ✓ Théorème de Gauss
- ✓ Calcul du PGCD et du PPCM
- ✓ Congruences modulo n
- ✓ Équations diophantiennes

FORMULES À RETENIR

- $a = bq + r$ avec $0 \leq r < |b|$
- $\gcd(a, b) \times \text{ppcm}(a, b) = |ab|$
- $au + bv = \gcd(a, b)$
- $a \equiv b \pmod{n} \iff n \mid (a - b)$
- $ax + by = c$ (solutions entières si $\gcd(a, b) \mid c$)

14 CLASSES D'ÉQUIVALENCE DANS $\mathbb{Z}/n\mathbb{Z}$

Relation de congruence :

$$a \equiv b \pmod{n}$$

C'est une relation d'équivalence (réflexive, symétrique, transitive).

15 CLASSE D'ÉQUIVALENCE DE a

La classe d'équivalence de a modulo n est :

$$\bar{a} = \{ k \in \mathbb{Z} / k \equiv a \pmod{n} \}$$

On la note : $\bar{a}$ ou $a + n\mathbb{Z}$

Exemple dans $\mathbb{Z}/5\mathbb{Z}$:

$$\bar{2} = \{ \dots, -8, -3, 2, 7, 12, \dots \}$$

16 ENSEMBLE QUOTIENT $\mathbb{Z}/n\mathbb{Z}$

L'ensemble des classes d'équivalence modulo n est :

$$\mathbb{Z}/n\mathbb{Z} = \{ \bar{0}, \bar{1}, \bar{2}, \dots, \bar{n-1} \}$$

Il contient exactement n classes.

Exemple : $\mathbb{Z}/4\mathbb{Z} = \{ \bar{0}, \bar{1}, \bar{2}, \bar{3} \}$

17 ÉGALITÉ DE DEUX CLASSES

Deux classes sont égales si :

$$\bar{a} = \bar{b} \iff a \equiv b \pmod{n}$$

Exemple dans $\mathbb{Z}/6\mathbb{Z}$:

$$\bar{8} = \bar{2} \quad \text{car} \quad 8 \equiv 2 \pmod{6}$$

18 OPÉRATIONS DANS $\mathbb{Z}/n\mathbb{Z}$

- Addition : $\bar{a} + \bar{b} = \overline{a + b}$
- Multiplication : $\bar{a} \times \bar{b} = \overline{ab}$
- Opposé : $-\bar{a} = \overline{-a}$
- Neutres : $\bar{0}$ (pour +), $\bar{1}$ (pour $\times$)

19 INVERSIBLE DANS $\mathbb{Z}/n\mathbb{Z}$

$\bar{a}$ est inversible s'il existe $\bar{b}$ telle que :

$$\bar{a} \times \bar{b} = \bar{1}$$

Condition fondamentale :

$$\bar{a} \text{ est inversible} \iff \gcd(a, n) = 1$$

Exemple dans $\mathbb{Z}/7\mathbb{Z}$:

$$\bar{3}^{-1} = \bar{5} \quad \text{car} \quad 3 \times 5 = 15 \equiv 1 \pmod{7}$$

20 RÉOLUTION D'ÉQUATIONS DANS $\mathbb{Z}/n\mathbb{Z}$

Exemple : $\bar{3}x = \bar{2}$ dans $\mathbb{Z}/7\mathbb{Z}$

Comme $\bar{3}^{-1} = \bar{5}$, on multiplie par $\bar{5}$:

$$x = \bar{5} \times \bar{2} = \bar{10} = \bar{3}$$

Donc $x = \bar{3}$

CONSEILS POUR LE BAC

- ✓ Bien maîtriser les démonstrations.
- ✓ Toujours utiliser : Bézout, Gauss, divisibilité et congruences.
- ✓ Vérifier les conditions avant d'appliquer un théorème.
- ✓ Soigner la rédaction logique.

RÉSUMÉ RAPIDE

- $a \equiv b \pmod{n} \iff n \mid (a - b)$
- $\mathbb{Z}/n\mathbb{Z} = \{ \bar{0}, \bar{1}, \dots, \bar{n-1} \}$
- $\bar{a} = \bar{b} \iff a \equiv b \pmod{n}$
- $\bar{a} + \bar{b} = \overline{a + b}$
- $\bar{a} \times \bar{b} = \overline{ab}$
- $\bar{a}$ inversible $\iff \gcd(a, n) = 1$
- $ax + by = c$ (solutions si $\gcd(a, b) \mid c$)

EXEMPLE COMPLET RAPIDE

Dans $\mathbb{Z}/5\mathbb{Z}$:

- Classes : $\{ \bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4} \}$
- $\bar{2} + \bar{4} = \bar{6} = \bar{1}$
- $\bar{2} \times \bar{3} = \bar{6} = \bar{1}$
- Inversibles : $\bar{1}, \bar{2}, \bar{3}, \bar{4}$ (car $\gcd(k, 5) = 1$)
- $\bar{2}^{-1} = \bar{3}$ car $2 \times 3 = 6 \equiv 1 \pmod{5}$

EXERCICES



Exercice 1

- 1) Calculer le reste de 7^{2026} dans la division par 10.
- 2) En déduire que $7^{2026} + 3^{2026}$ est divisible par 10.

Exercice 2

Montrer que $11^{2025} - 1$ est divisible par 10.

Exercice 3

- 1) Calculer le reste de 5^{2024} dans la division par 7.
- 2) En déduire que $5^{2024} + 2$ est divisible par 7.

Exercice 4

Montrer que pour tout entier naturel n :
 $3^{2n} - 1$ est divisible par 8.

Exercice 5

- 1) Montrer que $17^4 \equiv 1 [16]$.
- 2) En déduire le reste de 17^{2025} dans la division par 16.

Exercice 6 (défi Bac)

Soit n un entier naturel.

Montrer que :

$(2^n - 1)(2^n + 1)$ est divisible par 3.

RAPPEL RAPIDE

- ✓ $a \equiv b [n] \Leftrightarrow a - b$ est divisible par n
- ✓ $a^k \equiv b^k [n]$
- ✓ $A \equiv 0 [n] \Rightarrow n$ divise A

CORRIGÉS



Exercice 1

- 1) $7^2 \equiv 9 [10]$; donc $7^4 \equiv 1 [10]$.
 $2026 = 4 \times 506 + 2$
 $7^{2026} \equiv 7^2 \equiv 9 [10]$.
2) De même, $3^2 \equiv 9 [10]$ donc $3^4 \equiv 1 [10]$.
Donc $3^{2026} \equiv 9 [10]$.
Ainsi $7^{2026} + 3^{2026} \equiv 9 + 9 \equiv 18 \equiv 0 [10]$.
Donc $7^{2026} + 3^{2026}$ est **divisible par 10**.

Reste = 9

Exercice 2

On a $11 \equiv 1 [10]$ donc $11^{2025} \equiv 1^{2025} \equiv 1 [10]$.
Alors $11^{2025} - 1 \equiv 1 - 1 \equiv 0 [10]$.
Donc $11^{2025} - 1$ est **divisible par 10**.

Exercice 3

- 1) $5^1 \equiv 5 [7]$; $5^2 \equiv 4 [7]$; $5^3 \equiv 6 [7]$
 $5^4 \equiv 2 [7]$; $5^5 \equiv 3 [7]$; $5^6 \equiv 1 [7]$.
Le cycle est : 5, 4, 6, 2, 3, 1 de longueur 6.
 $2024 = 6 \times 337 + 2$ donc
 $5^{2024} \equiv 5^2 \equiv 4 [7]$.
2) $5^{2024} + 2 \equiv 4 + 2 \equiv 6 \equiv -1 [7]$.
Or $-1 \equiv 6 [7]$. Donc $5^{2024} + 2$ est **divisible par 7**.

Reste = 4

Exercice 4

$3^2 \equiv 9 \equiv 1 [8]$. Donc $(3^2)^n \equiv 1^n \equiv 1 [8]$
Alors $3^{2n} - 1 \equiv 1 - 1 \equiv 0 [8]$.
Donc $3^{2n} - 1$ est **divisible par 8**.

Exercice 5

- 1) $17^2 = 289 \equiv 1 [16]$ donc $17^4 = (17^2)^2 \equiv 1^2 \equiv 1 [16]$.
- 2) Comme $17^4 \equiv 1 [16]$, le cycle a longueur 4.
 $2025 = 4 \times 506 + 1$ donc
 $17^{2025} \equiv 17^1 \equiv 17 \equiv 1 [16]$.

Reste = 1

Exercice 6 (défi Bac)

$(2^n - 1)(2^n + 1) = 2^{2n} - 1$.
Or $2 \equiv -1 [3]$ donc $2^{2n} \equiv (-1)^{2n} \equiv 1 [3]$.
Ainsi $2^{2n} - 1 \equiv 1 - 1 \equiv 0 [3]$.
Donc $(2^n - 1)(2^n + 1)$ est **divisible par 3**.

Resoudre dans $\mathbb{Z}$ le système d'équation

$$\begin{cases} x \equiv 1[3] \\ x \equiv 2[7] \end{cases}$$

Résolution

Resolons dans $\mathbb{Z}$ le système d'équation

$$\begin{cases} x \equiv 1[3] \Rightarrow \exists k \in \mathbb{Z} ; x = 3k + 1 \\ x \equiv 2[7] \Rightarrow \exists k' \in \mathbb{Z} ; x = 7k' + 2 \end{cases}$$

Par Comparaison On a :

$$3k + 1 \equiv 7k' + 2 \iff 3k - 7k' = 1$$

On sait que ; $f \equiv 3 \times 2 + 1$ **MATHS S**

$$3 \times 2 - 7 = -1$$

$$3 \times (-2) - 7(-1) = 1 \quad - - (1)$$

$$3k - 7k' = 1 \quad - - - (2)$$

Faisons la différence (2) - (1) membre à membre

$$3k - 7k' + 3(2) + 7(-1) = 0$$

$$3(k + 2) - 7(k' + 1) = 0 \iff 3(k + 2) = 7(k' + 1)$$

On sait que $\text{pgcd}(3; 7) = 1$ alors d'après le

Théorème de Gauss, On a :

$$\begin{aligned} & \begin{cases} k + 2 \equiv 7\lambda \\ k' + 1 \equiv 3\lambda \end{cases} \quad \text{avec } \lambda \in \mathbb{Z} \\ \implies & \begin{cases} k = 7\lambda - 2 \\ k' = 3\lambda - 1 \end{cases} \quad \text{Ainsi } x = 3(7\lambda - 2) + 1 \\ \implies & \boxed{\boxed{x = 21\lambda - 5}} ; \text{ ou } \lambda \in \mathbb{Z} \end{aligned}$$

Exercice 8

I) Soit n un entier naturel.

1 Déterminer suivant les valeurs de n le reste de la division euclidienne de 9^n par 13.

2 On pose $a_n = (n - 1) \cdot 9^n + n \cdot 9^{n+1} + (n + 1) \cdot 9^{n+2}$ et $S = \sum_{k=0}^{400} a_k$

a Montrer que $a_n \equiv 2 \times 9^n \pmod{13}$.

b Prouver que $4S - 9^{401} \equiv 12 \pmod{13}$

c En déduire le reste de la division euclidienne de S par 13.

II) On considère dans $\mathbb{N}^* \times \mathbb{N}^*$ l'équation : (E) : $13^x - 4^y = 9$

1 Déterminer x lorsque $y = 1$.

On considère (x, y) une solution de (E) tel que $y \geq 2$.

2 Montrer que $5^x \equiv 1 \pmod{8}$ et déduire que x est pair. On pose $x = 2k$, $k \in \mathbb{N}^*$.

3 a Vérifier que les nombres $13^k - 3$ et $13^k + 3$ sont pairs.

b Montrer qu'il existe deux entiers naturels a et b tels que $2^a = 13^k - 3$ et $2^b = 13^k + 3$.

c En déduire que $a = 1$ et $b = 3$.

4 Résoudre alors l'équation (E).