COURS ILLUSTRÉ - LYCÉE - 2ÈME BAC SCIENCES MATHÉMATIQUES A - SEMESTRE 2

Arithmétique

L'arithmétique étudie les entiers, leurs diviseurs et les restes des divisions. En 2 Bac SM A, on apprend à écrire et calculer dans une base quelconque, à décomposer un entier en facteurs premiers, à relier l'algorithme d'Euclide aux identités de Bézout, puis à utiliser le théorème de Gauss et les congruences pour résoudre des équations dans $\mathbb{Z}$. Les classes modulo n, le petit théorème de Fermat et un exemple de codage complètent ce cours d'arithmétique dans $\mathbb{Z}$, suivi de six exercices corrigés.

Mathématiques 2ème Bac Sciences Mathématiques A BIOF - Programme marocain - Mis à jour le 18/11/2026

Objectifs du chapitre

- Écrire, comparer et calculer dans un système de numération de base b
- Déterminer PGCD, PPCM et diviseurs grâce à la décomposition en facteurs premiers
- Appliquer Euclide, Bézout et Gauss, et résoudre l'équation $ax + by = c$ dans $\mathbb{Z}^2$
- Calculer avec les congruences, dans $\mathbb{Z}/n\mathbb{Z}$, et utiliser le petit théorème de Fermat

Avant de commencer

- Divisibilité, nombres premiers et division euclidienne vus en 1ère Bac SM
- Identités remarquables et raisonnement par récurrence
- Calcul dans les entiers relatifs

1. Divisibilité et division euclidienne dans $\mathbb{Z}$

Divisibilité

Pour des entiers a et b, écrire $a \mid b$ signifie qu'il existe $k \in \mathbb{Z}$ tel que $b = ak$: on dit que a divise b, ou que b est un multiple de a. Si a divise b et c, il divise toute combinaison $ub + vc$ avec $u, v \in \mathbb{Z}$. Si $a \mid b$ et $b \mid c$, alors $a \mid c$.

Division euclidienne

Pour tout entier a et tout entier $b > 0$, il existe un unique couple d'entiers (q, r) tel que $a = bq + r$ et $0 \leq r < b$. Les entiers q et r sont le quotient et le reste ; les contraintes sur le reste font partie du résultat.

Un dividende négatif

$-17 = 5 \times (-4) + 3$ est la division euclidienne de -17 par 5 : le reste vaut 3.

1. L'écriture $-17 = 5 \times (-3) - 2$ est une égalité correcte, mais son reste négatif ne satisfait pas la définition.

2. Systèmes de numération en base b

Écriture positionnelle

Dans une base entière $b \geq 2$, tout entier naturel non nul s'écrit de manière unique $N = a_k b^k + \cdots + a_1 b + a_0$, où chaque chiffre vérifie $0 \leq a_j \leq b - 1$ et $a_k \neq 0$. On note cette écriture $\overline{a_k \cdots a_1 a_0}^{(b)}$, ou $(a_k \cdots a_0)_b$.

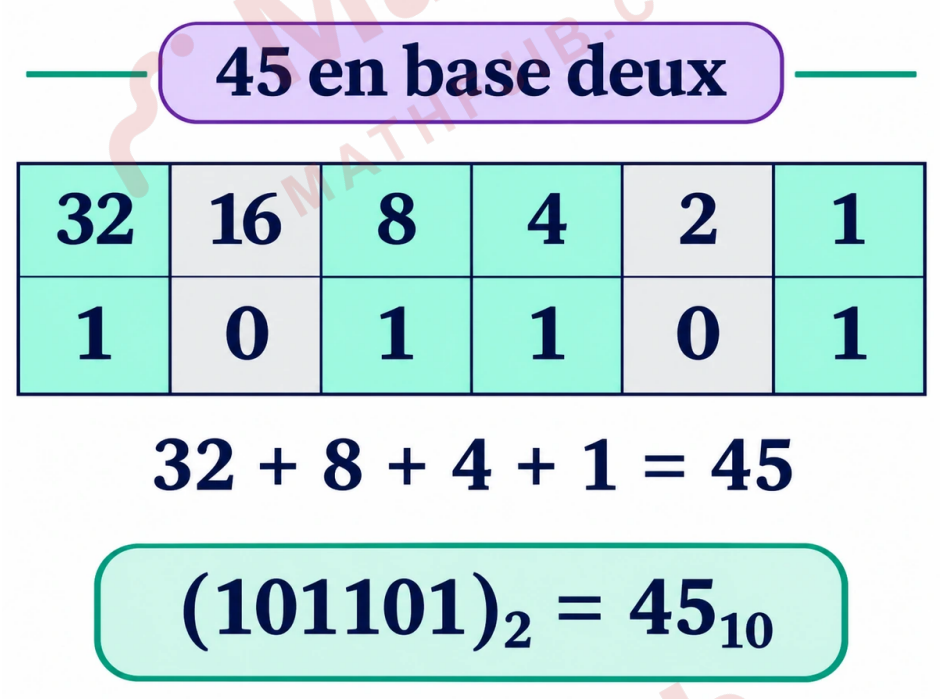
Méthode : Convertir depuis la base dix

1. Diviser successivement le nombre, puis les quotients obtenus, par la base choisie, jusqu'à obtenir un quotient nul.
2. Noter les restes, tous compris entre 0 et $b-1$.
3. Lire les restes du dernier au premier ; vérifier par la somme des puissances de la base.

Écrire 45 en binaire

Les divisions successives par 2 donnent les couples quotient et reste $(22,1)$, $(11,0)$, $(5,1)$, $(2,1)$, $(1,0)$, $(0,1)$.

1. En lisant les restes à l'envers : $45=(101101)_2=32+8+4+1$. En base 2, $(1011)_2+(110)_2=(10001)_2$ et $(101)_2\times(11)_2=(1111)_2$: les retenues se font à partir de 2, et non de 10.



Le nombre $(101101)_2$ vaut $1\times32+0\times16+1\times8+1\times4+0\times2+1\times1=45$ en base dix.

Passer d'une base à l'autre et comparer

$(243)_5=2\times5^2+4\times5+3=73$ en base dix.

1. Pour comparer deux entiers écrits dans la même base, sans zéro à gauche, celui qui a le plus de chiffres est le plus grand ; à nombre de chiffres égal, on compare les chiffres de gauche à droite. Ainsi $(2101)_3>(1222)_3$, ce que confirment les valeurs 64 et 53.

3. Nombres premiers et théorème fondamental

Nombre premier

Un entier $p\geq2$ est premier si ses seuls diviseurs positifs sont 1 et p. Le nombre 1 n'est pas premier. Tout entier $n\geq2$ non premier possède un diviseur premier p tel que $p^2\leq n$: pour tester la primalité de n, il suffit de chercher un diviseur premier inférieur ou égal à $\sqrt{n}$.

Le crible d'Ératosthène élimine les multiples des nombres premiers successifs pour obtenir tous les nombres premiers inférieurs à un entier donné. L'ensemble des nombres premiers est infini : si l'on supposait qu'il n'y en a qu'un

nombre fini $p_1, \ldots, p_k$, le nombre $N = p_1 \cdots p_k + 1$ aurait un diviseur premier, qui diviserait aussi $p_1 \cdots p_k$, donc $N - p_1 \cdots p_k = 1$, ce qui est impossible.

Théorème fondamental de l'arithmétique

Tout entier $n \geq 2$ se décompose en produit de facteurs premiers $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, où $p_1 < p_2 < \cdots < p_k$ sont premiers et $\alpha_j \geq 1$. Cette décomposition est unique.

Diviseurs, PGCD et PPCM par la décomposition

Les diviseurs positifs de $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ sont les entiers $p_1^{\beta_1} \cdots p_k^{\beta_k}$ avec $0 \leq \beta_j \leq \alpha_j$; ils sont au nombre de $(\alpha_1 + 1) \cdots (\alpha_k + 1)$. Pour deux entiers non nuls, le PGCD utilise les facteurs communs avec leurs exposants minimaux, et le PPCM tous les facteurs avec leurs exposants maximaux. On a $\text{PGCD}(a, b) \times \text{PPCM}(a, b) = |ab|$.

Séparer facteurs communs et facteurs nécessaires

$180 = 2^2 \times 3^2 \times 5$ et $84 = 2^2 \times 3 \times 7$. Leur PGCD vaut $2^2 \times 3 = 12$ et leur PPCM $2^2 \times 3^2 \times 5 \times 7 = 1260$; le produit 12×1260 vaut bien $180 \times 84 = 15120$.

1. L'entier 180 possède $(2+1)(2+1)(1+1) = 18$ diviseurs positifs.

4. PGCD, algorithme d'Euclide et identité de Bézout

Propriétés du PGCD

On note $a \wedge b$ le PGCD de deux entiers non tous deux nuls. Un entier divise a et b si et seulement s'il divise $a \wedge b$. Pour $k \neq 0$, $(ka) \wedge (kb) = |k|\,(a \wedge b)$. Si $d = a \wedge b$, on peut écrire $a = da'$ et $b = db'$ avec $a' \wedge b' = 1$. Deux entiers sont premiers entre eux si leur PGCD vaut 1.

Conservation du PGCD

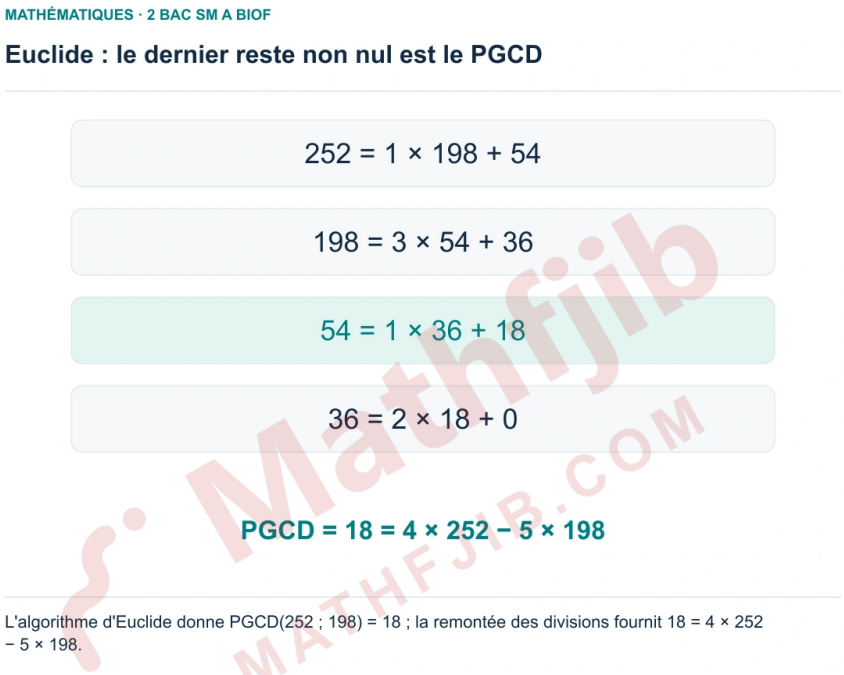
Si $a = bq + r$, alors $a \wedge b = b \wedge r$. En répétant les divisions euclidiennes, le dernier reste non nul est le PGCD : c'est l'algorithme d'Euclide.

Remonter les divisions

$252 = 198 + 54$, $198 = 3 \times 54 + 36$, $54 = 36 + 18$, $36 = 2 \times 18$. Le PGCD vaut donc 18.

1. En remontant : $18 = 54 - 36 = 54 - (198 - 3 \times 54) = 4 \times 54 - 198 = 4 \times (252 - 198) - 198 = 4 \times 252 - 5 \times 198$. On obtient des coefficients de Bézout en même temps que le PGCD.

Mathfjib MATHFJIB.COM



L'algorithme d'Euclide donne $252 \wedge 198 = 18$; la remontée des divisions fournit $18 = 4 \times 252 - 5 \times 198$.

Théorème de Bézout

Pour deux entiers a et b non tous deux nuls, il existe $u, v \in \mathbb{Z}$ tels que $au + bv = a \wedge b$. En particulier, a et b sont premiers entre eux si et seulement s'il existe $u, v \in \mathbb{Z}$ tels que $au + bv = 1$.

5. Théorème de Gauss et équations diophantiennes

Théorème de Gauss

Si $a \mid bc$ et si $a \wedge b = 1$, alors $a \mid c$.

L'hypothèse de coprimalité est indispensable : 6 divise 2×3, mais ne divise ni 2 ni 3. Pour démontrer Gauss à l'aide de Bézout, on écrit $au + bv = 1$, puis on multiplie par c : $c = acu + bcv$, et a divise chacun des deux termes.

Conséquences de Gauss

Si un nombre premier p divise un produit ab, alors $p \mid a$ ou $p \mid b$. Si $a \mid n$, $b \mid n$ et $a \wedge b = 1$, alors $ab \mid n$. Si $a \wedge b = 1$ et $a \wedge c = 1$, alors $a \wedge (bc) = 1$.

Résolution de $ax + by = c$

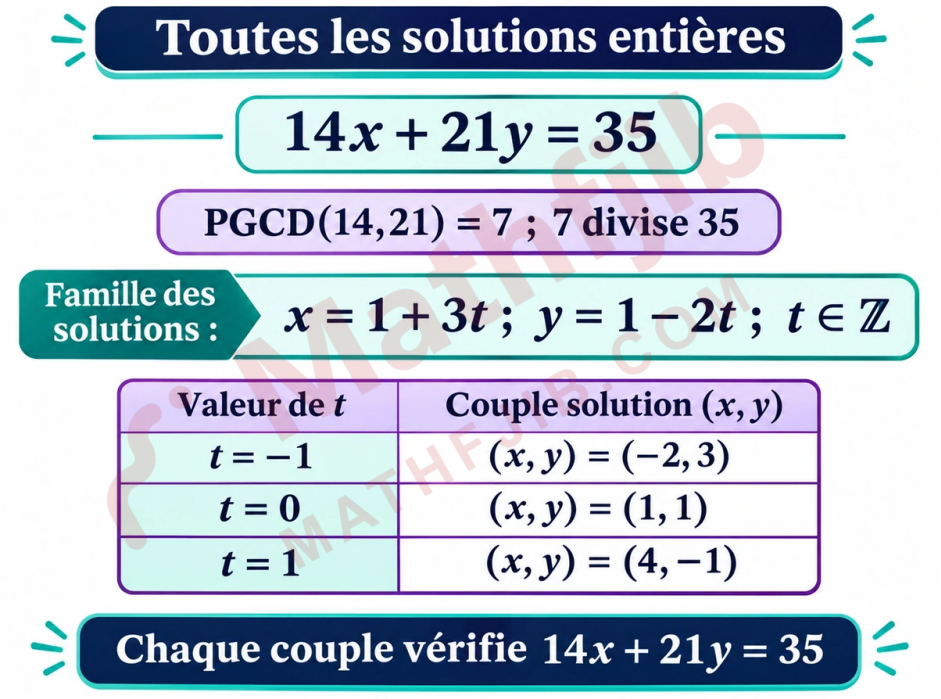
Soient a et b non nuls et $d = a \wedge b$. L'équation $ax + by = c$ admet des solutions dans $\mathbb{Z}^2$ si et seulement si $d \mid c$. Si (x_0, y_0) est une solution, toutes les solutions sont les couples $\left(x_0 + \dfrac{b}{d}t,\ y_0 - \dfrac{a}{d}t\right)$, avec $t \in \mathbb{Z}$.

Pour établir la forme générale, on soustrait : $a(x - x_0) = -b(y - y_0)$, puis on divise par d ; comme $\dfrac{a}{d}$ et $\dfrac{b}{d}$ sont premiers entre eux, Gauss donne $\dfrac{b}{d} \mid x - x_0$. On écrit $x - x_0 = \dfrac{b}{d}t$ et l'on en déduit y.

Décrire toutes les solutions, pas seulement une

Pour $14x + 21y = 35$, le PGCD vaut 7 et divise 35. Le couple $(1, 1)$ est une solution.

1. Toutes les solutions sont $x = 1 + 3t$, $y = 1 - 2t$, avec $t \in \mathbb{Z}$. Si l'on exige $x \geq 0$ et $y \geq 0$, il faut $t \geq 0$ et $t \leq 0$: seul le couple $(1, 1)$ convient.



Toutes les solutions entières de $14x + 21y = 35$ sont $x = 1 + 3t$ et $y = 1 - 2t$, pour $t \in \mathbb{Z}$.

6. Congruences modulo n : calculer sur les restes

Congruence

Pour $n \geq 2$, $a \equiv b\ [n]$ signifie que $n \mid (a - b)$. Deux entiers sont congrus modulo n si et seulement s'ils ont le même reste dans la division euclidienne par n.

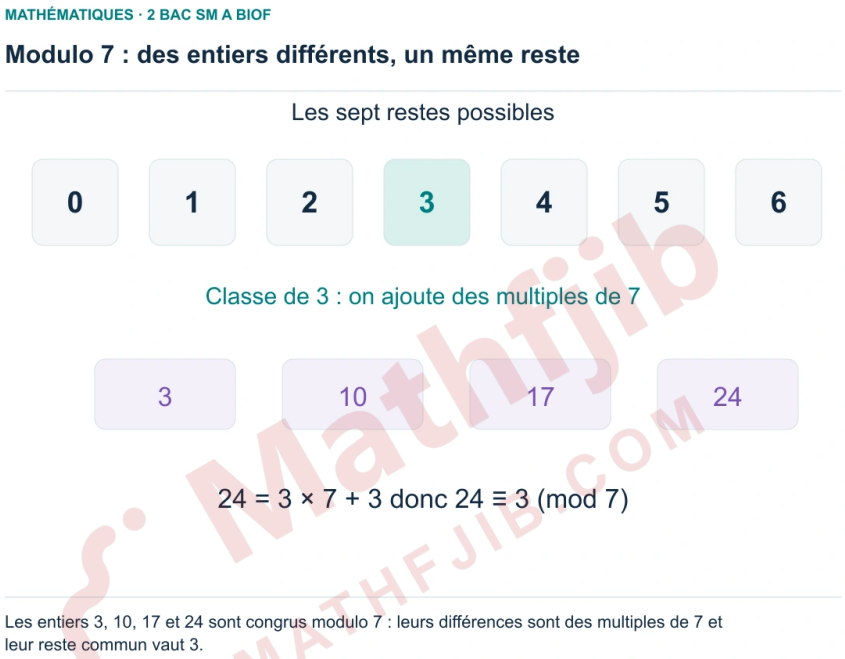
Opérations autorisées

Si $a \equiv b\ [n]$ et $c \equiv d\ [n]$, alors $a + c \equiv b + d\ [n]$, $ac \equiv bd\ [n]$ et $a^k \equiv b^k\ [n]$ pour tout entier $k \geq 0$. On peut simplifier un facteur c seulement si $c \wedge n = 1$: en général, une division n'est pas autorisée.

Une simplification impossible

Modulo 6, $2 \times 1 \equiv 2 \times 4$, puisque les deux produits ont pour reste 2.

1. Pourtant 1 et 4 ne sont pas congrus modulo 6 : le facteur 2 n'est pas inversible modulo 6.



Les entiers 3, 10, 17 et 24 sont congrus modulo 7 : leurs différences sont des multiples de 7 et leur reste commun vaut 3.

Critères de divisibilité

Comme $10 \equiv 1\ [9]$, on a $10^k \equiv 1\ [9]$: un entier est congru modulo 9, et modulo 3, à la somme de ses chiffres. Ainsi $7425 \equiv 7+4+2+5 = 18 \equiv 0\ [9]$.

1. Comme $10 \equiv -1\ [11]$, un entier est congru modulo 11 à la somme alternée de ses chiffres en partant des unités : $7425 \equiv 5-2+4-7 = 0\ [11]$, donc $11 \mid 7425$.

Méthode : Raisonner avec un tableau de restes

1. Lister les restes possibles de x modulo n.
2. Calculer le reste de l'expression étudiée pour chacun d'eux.
3. Conclure : par exemple, $x^2 \equiv 0$ ou $1\ [4]$ pour tout entier x, donc une somme de deux carrés n'est jamais congrue à 3 modulo 4.

6.1 Les classes $\mathbb{Z}/n\mathbb{Z}$ et l'inverse modulaire

La classe $\overline{a}$ regroupe les entiers congrus à a modulo n. L'ensemble $\mathbb{Z}/n\mathbb{Z}$ contient exactement n classes, $\overline{0}, \overline{1}, \ldots, \overline{n-1}$. On y définit $\overline{a}+\overline{b} = \overline{a+b}$ et $\overline{a}\times\overline{b} = \overline{ab}$; ces opérations ne dépendent pas des représentants choisis. Une classe $\overline{a}$ possède un inverse multiplicatif si et seulement si $a \wedge n = 1$, et Bézout permet de le construire.

Résoudre une congruence linéaire

Pour $5x \equiv 3\ [11]$, on remarque que $5\times 9 = 45 \equiv 1\ [11]$: $\overline{9}$ est l'inverse de $\overline{5}$ dans $\mathbb{Z}/11\mathbb{Z}$.

1. En multipliant par 9 : $x \equiv 27 \equiv 5\ [11]$. Les solutions sont les entiers $x = 5+11t$, avec $t \in \mathbb{Z}$.

Le cas d'un module premier

Si p est premier, toute classe non nulle de $\mathbb{Z}/p\mathbb{Z}$ est inversible, car $a \wedge p = 1$ dès que $p \nmid a$. Dans $\mathbb{Z}/p\mathbb{Z}$, un produit de classes est nul seulement si l'une d'elles est nulle, et l'on peut simplifier par toute classe non nulle.

7. Petit théorème de Fermat

Petit théorème de Fermat

Si p est premier et si $p \nmid a$, alors $a^{p-1} \equiv 1\ [p]$. Pour tout entier a, on a aussi $a^p \equiv a\ [p]$.

Idée de preuve : si $p \nmid a$, la multiplication par $\overline{a}$ permute les classes non nulles $\overline{1}, \ldots, \overline{p-1}$ de $\mathbb{Z}/p\mathbb{Z}$. Le produit P de ces classes est donc égal au produit des classes $\overline{ka}$, qui vaut $\overline{a}^{p-1}P$; comme P est inversible dans $\mathbb{Z}/p\mathbb{Z}$, on obtient $\overline{a}^{p-1} = \overline{1}$. L'hypothèse « p premier » est nécessaire dans cet énoncé.

Réduire une grande puissance

Comme 7 est premier et ne divise pas 3, $3^6 \equiv 1\ [7]$. Or $100 = 16 \times 6 + 4$, donc $3^{100} = (3^6)^{16} \times 3^4 \equiv 3^4 = 81 \equiv 4\ [7]$.

1. Fermat fournit une congruence lorsque la primalité est connue ; une congruence de ce type ne suffit pas, à elle seule, à prouver qu'un entier est premier.

8. Une application de codage par congruences

Coder puis retrouver une lettre

On numérote les lettres de 0 à 25 et l'on code par $y \equiv 5x + 8\ [26]$. Comme $5 \wedge 26 = 1$ et $5 \times 21 = 105 \equiv 1\ [26]$, on décode par $x \equiv 21(y - 8)\ [26]$.

1. Pour la lettre de numéro 2, le code vaut 18. Le décodage donne $21 \times (18-8) = 210 \equiv 2\ [26]$. Ce chiffrement affine illustre l'inverse modulaire ; ce n'est pas un procédé de sécurité moderne.

Remarque

La notation $a \wedge b$ du PGCD est celle des manuels marocains ; on rencontre aussi $\text{PGCD}(a, b)$. Le PPCM se note parfois $a \vee b$.

Je retiens

- La division euclidienne exige un reste positif ou nul, strictement inférieur au diviseur.
- Tout entier $n \geq 2$ se décompose de façon unique en facteurs premiers ; $p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ a $(\alpha_1 + 1) \cdots (\alpha_k + 1)$ diviseurs positifs.
- Euclide calcule le PGCD ; la remontée des divisions donne des coefficients de Bézout.
- Gauss : si $a \mid bc$ et $a \wedge b = 1$, alors $a \mid c$.
- $ax + by = c$ a des solutions entières si et seulement si $a \wedge b$ divise c ; on décrit ensuite toutes les solutions.
- Dans une congruence modulo n, on ne simplifie un facteur que s'il est premier avec n.
- Fermat : si p est premier et $p \nmid a$, alors $a^{p-1} \equiv 1\ [p]$.

Exercices - À chercher avant la correction

Cherchez chaque exercice sur votre cahier avant de lire sa correction. Justifiez chaque étape et citez le théorème utilisé, avec ses hypothèses.

Exercice 1. Calculer dans une base

Facile

1. Écrire 2026 en base 5.
2. Calculer $(1101)_2 + (111)_2$ en base 2, puis vérifier en base dix.
3. Comparer $(2101)_3$ et $(1222)_3$ sans les convertir, puis vérifier.

Exercice 2. Décomposition, PGCD, PPCM et diviseurs

Facile

1. Décomposer 360 et 84 en produits de facteurs premiers.
2. En déduire $360 \wedge 84$ et le PPCM de 360 et 84.
3. Combien 360 possède-t-il de diviseurs positifs ?

Exercice 3. Un problème de monnaie

Intermédiaire

Un commerçant vend deux articles, l'un à 23 DH et l'autre à 7 DH. Une cliente paie exactement 100 DH. On cherche les nombres x et y d'articles achetés.

1. Avec l'algorithme d'Euclide, déterminer $23 \wedge 7$ et des entiers u, v tels que $23u + 7v = 1$.
2. Résoudre dans $\mathbb{Z}^2$ l'équation $23x + 7y = 100$.
3. En déduire la réponse au problème.

Exercice 4. Congruences et restes

Intermédiaire

1. Déterminer le chiffre des unités de 7^{2026}.
2. Montrer que, pour tout entier naturel n, $3^{2n} - 2^n$ est divisible par 7.
3. Montrer que le carré d'un entier est congru à 0 ou à 1 modulo 4. L'entier 2027 peut-il être la somme de deux carrés ?

Exercice 5. Un système de congruences

Approfondissement

On cherche les entiers x tels que $x \equiv 2\ [5]$ et $x \equiv 3\ [7]$.

1. Montrer que x convient si et seulement si $x = 2 + 5k$ avec $5k \equiv 1\ [7]$.
2. Déterminer l'inverse de 5 modulo 7 et en déduire toutes les solutions.
3. Quelle est la plus petite solution supérieure à 100 ?

Exercice 6. Fermat et divisibilité par 42

Approfondissement

1. Montrer que, pour tout entier n, $n^7 - n$ est divisible par 7.
2. Montrer que $n^7 - n$ est aussi divisible par 2 et par 3, puis par 42.
3. Résoudre dans $\mathbb{Z}$ les congruences $3x \equiv 5\ [7]$ et $x^2 \equiv 2\ [7]$.

Mathfjib MATHFJIB.COM
Mathfjib MATHFJIB.COM

Corrections expliquées des exercices

Exercice 1. Calculer dans une base

1. $2026 = 5 \times 405 + 1$, $405 = 5 \times 81 + 0$, $81 = 5 \times 16 + 1$, $16 = 5 \times 3 + 1$ et $3 = 5 \times 0 + 3$. En lisant les restes à l'envers : $2026 = (31101)_5$. Contrôle : $3 \times 625 + 125 + 25 + 1 = 2026$.

2. En posant l'addition avec des retenues de 2 : $(1101)_2 + (111)_2 = (10100)_2$. En base dix : $13 + 7 = 20 = 16 + 4$.

3. Les deux nombres ont quatre chiffres et le premier commence par $2 > 1$: $(2101)_3 > (1222)_3$. En base dix, ils valent $2 \times 27 + 9 + 1 = 64$ et $27 + 18 + 6 + 2 = 53$.

Exercice 2. Décomposition, PGCD, PPCM et diviseurs

1. $360 = 2^3 \times 3^2 \times 5$ et $84 = 2^2 \times 3 \times 7$.

2. $360 \wedge 84 = 2^2 \times 3 = 12$ et leur PPCM vaut $2^3 \times 3^2 \times 5 \times 7 = 2520$. Contrôle : $12 \times 2520 = 30240 = 360 \times 84$.

3. 360 possède $(3+1)(2+1)(1+1) = 24$ diviseurs positifs.

Exercice 3. Un problème de monnaie

1. $23 = 3 \times 7 + 2$, $7 = 3 \times 2 + 1$: le PGCD vaut 1. En remontant : $1 = 7 - 3 \times 2 = 7 - 3(23 - 3 \times 7) = 10 \times 7 - 3 \times 23$, donc $u = -3$ et $v = 10$.

2. En multipliant par 100 : $(-300, 1000)$ est une solution. Comme $23 \wedge 7 = 1$, toutes les solutions sont $x = -300 + 7t$ et $y = 1000 - 23t$, avec $t \in \mathbb{Z}$.

3. Il faut $x \geq 0$ et $y \geq 0$: $t \geq \dfrac{300}{7} \approx 42{,}9$ et $t \leq \dfrac{1000}{23} \approx 43{,}5$, donc $t = 43$. La cliente a acheté 1 article à 23 DH et 11 articles à 7 DH : $23 + 77 = 100$.

Exercice 4. Congruences et restes

1. Modulo 10 : $7^1 \equiv 7$, $7^2 \equiv 9$, $7^3 \equiv 3$, $7^4 \equiv 1$. Comme $2026 = 4 \times 506 + 2$, $7^{2026} = (7^4)^{506} \times 7^2 \equiv 9\ [10]$: le chiffre des unités est 9.

2. $3^{2n} = 9^n$ et $9 \equiv 2\ [7]$, donc $9^n \equiv 2^n\ [7]$ et $3^{2n} - 2^n \equiv 0\ [7]$.

3. Un entier est congru à 0, 1, 2 ou 3 modulo 4, et les carrés correspondants sont congrus à 0, 1, 0, 1. Une somme de deux carrés est donc congrue à 0, 1 ou 2 modulo 4. Comme $2027 = 4 \times 506 + 3 \equiv 3\ [4]$, ce n'est pas une somme de deux carrés.

Exercice 5. Un système de congruences

1. La première condition équivaut à $x = 2 + 5k$ avec $k \in \mathbb{Z}$. La seconde devient $2 + 5k \equiv 3\ [7]$, soit $5k \equiv 1\ [7]$.

2. $5 \times 3 = 15 \equiv 1\ [7]$: l'inverse de 5 modulo 7 est 3. Donc $k \equiv 3\ [7]$, $k = 3 + 7t$, et $x = 2 + 5(3 + 7t) = 17 + 35t$, avec $t \in \mathbb{Z}$. Contrôle : $17 = 3 \times 5 + 2$ et $17 = 2 \times 7 + 3$.

3. $17 + 35t > 100$ impose $t \geq 3$: la solution cherchée est $17 + 105 = 122$.

Exercice 6. Fermat et divisibilité par 42

1. 7 est premier : le petit théorème de Fermat donne $n^7 \equiv n\ [7]$ pour tout entier n.

2. n^7 et n ont la même parité, donc $2 \mid n^7 - n$. Par Fermat avec $p = 3$, $n^3 \equiv n\ [3]$, d'où $n^7 = n^3 \times n^3 \times n \equiv n \times n \times n = n^3 \equiv n\ [3]$. Les entiers 2, 3 et 7 sont deux à deux premiers entre eux et divisent tous $n^7 - n$: par la conséquence du théorème de Gauss, leur produit 42 divise $n^7 - n$.

3. L'inverse de 3 modulo 7 est 5, car $15 \equiv 1\ [7]$: $x \equiv 25 \equiv 4\ [7]$. Pour la seconde, les carrés modulo 7 des restes $0, \ldots, 6$ sont 0, 1, 4, 2, 2, 4, 1 : $x^2 \equiv 2\ [7]$ si et seulement si $x \equiv 3$ ou $x \equiv 4\ [7]$.

Mathfjib MATHFJIB.COM

Questions fréquentes

Quand utiliser Bézout et quand utiliser Gauss ?

Bézout sert à caractériser deux entiers premiers entre eux, à construire un inverse modulaire ou à obtenir une solution particulière. Gauss permet ensuite de déduire une divisibilité à partir de cette coprimalité.

Comment trouver toutes les solutions de $ax + by = c$?

Vérifier que $d = a \wedge b$ divise c, construire une solution particulière avec Euclide, puis écrire $x = x_0 + \frac{b}{d}t$ et $y = y_0 - \frac{a}{d}t$ avec t entier, en justifiant cette forme par Gauss.

Comment calculer le nombre de diviseurs d'un entier ?

Décomposer l'entier en facteurs premiers $p_1^{\alpha_1} \cdots p_k^{\alpha_k}$; le nombre de diviseurs positifs vaut $(\alpha_1 + 1) \cdots (\alpha_k + 1)$. Par exemple, $360 = 2^3 \times 3^2 \times 5$ en a 24.

Pourquoi ne peut-on pas toujours diviser une congruence ?

Un entier possède un inverse modulo n seulement s'il est premier avec n. Sans cette propriété, une simplification peut ajouter ou supprimer des solutions, comme le montre $2 \times 1 \equiv 2 \times 4\ [6]$.

Comment utiliser le petit théorème de Fermat ?

Si p est premier et ne divise pas a, remplacer a^{p-1} par 1 modulo p : on divise l'exposant par $p - 1$ et on ne garde que le reste. Cela réduit une grande puissance à un petit calcul.

MATHFJIB - Mathématiques 2 Bac SM A
Suivez les consignes et la progression de votre professeur.
Retrouver le cours, ses illustrations et les exercices corrigés en ligne.