MORAJA3A

MATHS · PHYSIQUE-CHIMIE · SVT

a | b

a ≡ b [n]

COURS · 1ÈRE ANNÉE BAC SCIENCES MATHS · SEMESTRE 2 · ARITHMÉTIQUE

Arithmétique dans ℤ

الحسابيات في ℤ

p premier

Divisibilité, division euclidienne, congruences modulo n, nombres premiers, décomposition en facteurs premiers, nombre de diviseurs, PGCD, PPCM, algorithme d'Euclide et nombres premiers entre eux, expliqués pas à pas.

PGCD

Comprends. Entraîne-toi. Réussis.

Rédigé et vérifié par **Mohammed TAOUFIK**, professeur et fondateur de MORAJA3A

NIVEAU
1ère Bac — Sciences Mathématiques (BIOF)

CONTENU
Cours · Exemples · Pièges · 10 exercices + corrigés

PLATEFORME
moraja3a.app

Sommaire

فهرس الدرس

01	Divisibilité dans ℤ	قابلية القسمة في ℤ
02	Division euclidienne	القسمة الأقليدية
03	Congruences modulo n	الموافقة بتردد n
04	Nombres premiers	الأعداد الأولية
05	PGCD et PPCM	القاسم المشترك الأكبر والمضاعف المشترك الأصغر
06	Exercices (10 exercices gradués)	تمارين تطبيقية
07	Corrigés détaillés	التصحيح المفصل
08	Fiche résumé et lexique français–arabe	ملخص ومعجم المصطلحات

POURQUOI CE CHAPITRE EST IMPORTANT

L'arithmétique étudie les **nombres entiers** : divisibilité, restes, nombres premiers. C'est une partie très « logique » des mathématiques, où chaque résultat se démontre proprement. Les **congruences** permettent de calculer très vite le reste d'énormes nombres (comme 2^{2026} modulo 7).
L'arithmétique est la base de la **cryptographie** (cartes bancaires, messageries) et elle sera approfondie en 2ème Bac SM (théorèmes de Bézout et de Gauss, équations diophantiennes).

بالعربية 💡

الحسابيات تدرس **الأعداد الصحيحة**: القسمة، البواقي، الأعداد الأولية. **الموافقات** تمكن من حساب باقي أعداد ضخمة بسرعة. الحسابيات أساس **التشفير**، وستتعمق فيها في السنة الثانية باكالوريا علوم رياضية.

Comment utiliser ce cours

- **Définition** (encadré bleu) : ce qu'il faut savoir par cœur.
- **À retenir** (encadré vert) : la loi, la formule ou la méthode clé.
- **Exemple** (encadré doré) : une application corrigée pas à pas.
- **Piège** (encadré rouge) : l'erreur que font beaucoup d'élèves.
- **بالعربية** : une explication courte en arabe pour bien fixer l'idée.
- **Exercices** : énoncés classés APPLICATION APPROFONDISSEMENT TYPE EXAMEN ; tous les corrigés sont regroupés après les exercices.

1 Divisibilité dans ℤ

قابلية القسمة في ℤ

DÉFINITION — DIVISEUR, MULTIPLE

Soient a et b deux entiers relatifs. On dit que a **divise** b (ou que b est un **multiple** de a), et on note $a \mid b$, s'il existe un entier $k \in \mathbb{Z}$ tel que :

$$b = k \times a$$

Exemples : $3 \mid 12$; $-4 \mid 20$; $7 \nmid 15$. Tout entier divise 0 ; 1 et −1 divisent tout entier.

PROPRIÉTÉS

Pour $a, b, c \in \mathbb{Z}$:

- $a \mid a$ (réflexivité) ;
- si $a \mid b$ et $b \mid c$, alors $a \mid c$ (transitivité) ;
- si $a \mid b$ et $b \mid a$, alors $a = b$ ou $a = -b$;
- **combinaison linéaire** : si $a \mid b$ et $a \mid c$, alors $a \mid (bu + cv)$ pour tous $u, v \in \mathbb{Z}$;
- si $a \mid b$ et $b \neq 0$, alors $|a| \leq |b|$.

MÉTHODE — TROUVER LES N TELS QUE N + 3 DIVISE 2N + 11

On fait apparaître $n + 3$: $2n + 11 = 2(n + 3) + 5$.

Si $n + 3 \mid 2n + 11$, comme $n + 3 \mid 2(n + 3)$, alors $n + 3$ divise la différence 5. Donc $n + 3 \in \{-5 ; -1 ; 1 ; 5\}$, soit $n \in \{-8 ; -4 ; -2 ; 2\}$. Réciproquement, ces valeurs conviennent.

PARITÉ

Un entier est **pair** s'il s'écrit $2k$, **impair** s'il s'écrit $2k + 1$ ($k \in \mathbb{Z}$). Le produit de deux entiers consécutifs $n(n + 1)$ est toujours pair.

PIÈGE

$a \mid bc$ n'entraîne pas $a \mid b$ ou $a \mid c$: $6 \mid 4 \times 9$ mais $6 \nmid 4$ et $6 \nmid 9$. (C'est vrai si a est **premier**, voir plus loin.)

💡 بالعربية

نقول إن a **يقسم** b ونكتب $a \mid b$ إذا وجد عدد صحيح k بحيث $b = ka$. إذا كان a يقسم b و c فإنه يقسم كل **تأليفة خطية** $bu + cv$. هذه الخاصية مفيدة جدا في التمارين.

Division euclidienne

2 القسمة الأقليدية

THÉORÈME

Soient a ∈ ℤ et b ∈ ℕ*. Il existe un **unique** couple (q ; r) d'entiers tels que :

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

q est le **quotient** et r le **reste** de la division euclidienne de a par b. On a : b | a ⇔ r = 0.

EXEMPLES

- 2026 = 17 × 119 + 3 : quotient 119, reste 3.
- −50 = 7 × (−8) + 6 : quotient −8, reste 6 (et non −50 = 7 × (−7) − 1, car le reste doit être positif).

CONSÉQUENCE : RESTES POSSIBLES

Dans la division par b, il n'y a que b restes possibles : 0, 1, ..., b − 1. Tout entier s'écrit donc sous l'une des formes bk, bk + 1, ..., bk + b − 1. C'est la base du **raisonnement par disjonction des cas** en arithmétique.

EXEMPLE

Montrer que n(n + 1)(n + 2) est divisible par 3 pour tout n ∈ ℤ.

n s'écrit 3k, 3k + 1 ou 3k + 2. Dans le premier cas, 3 | n ; dans le deuxième, n + 2 = 3k + 3 ; dans le troisième, n + 1 = 3k + 3. Dans tous les cas, l'un des trois facteurs est multiple de 3. ∎

PIÈGE

Le reste doit vérifier 0 ≤ r < b. « 2026 = 17 × 118 + 20 » est vrai, mais ce n'est **pas** la division euclidienne car 20 ≥ 17.

💡 **بالعربية**

القسمة الأقليدية: لكل a من ℤ و b من ℕ* يوجد زوج وحيد (q ; r) بحيث a = bq + r مع 0 ≤ q. r < b هو **الخارج** و r هو **الباقي**. الباقي دائما موجب وأصغر من b.

3 Congruences modulo n

الموافقة بتردید n

DÉFINITION — CONGRUENCE

Soit n ∈ ℕ*. Deux entiers a et b sont **congrus modulo** n, et on note a ≡ b [n], si n divise a − b :

$$a \equiv b\ [n] \Leftrightarrow n \mid (a-b) \Leftrightarrow \text{a et b ont le même reste dans la division par n}$$

En particulier, a ≡ r [n] où r est le reste de la division de a par n, et n | a ⇔ a ≡ 0 [n].

EXEMPLES

17 ≡ 2 [5] ; −3 ≡ 4 [7] ; 100 ≡ 1 [9] ; 10 ≡ −1 [11].

COMPATIBILITÉ AVEC LES OPÉRATIONS

Si a ≡ b [n] et c ≡ d [n], alors :

$$a + c \equiv b + d\ [n]\ ;\ a - c \equiv b - d\ [n]\ ;\ ac \equiv bd\ [n]$$

$$a^k \equiv b^k\ [n] \text{ pour tout } k \in \mathbb{N}$$

On peut donc remplacer un nombre par un nombre plus simple qui lui est congru, dans les sommes, les produits et les puissances.

CALCULER LE RESTE DE 2^2026 MODULO 7

On cherche une puissance de 2 congrue à 1 : $2^3 = 8 \equiv 1\ [7]$.

$2026 = 3 \times 675 + 1$, donc $2^{2026} = (2^3)^{675} \times 2 \equiv 1^{675} \times 2 \equiv 2\ [7]$. Le reste est **2**.

CHIFFRE DES UNITÉS DE 7^2026

Le chiffre des unités est le reste modulo 10. $7^2 = 49 \equiv -1\ [10]$, donc $7^4 \equiv 1\ [10]$. $2026 = 4 \times 506 + 2$: $7^{2026} \equiv 7^2 \equiv 9\ [10]$. Le chiffre des unités est **9**.

CRITÈRES DE DIVISIBILITÉ (DÉMONTRÉS AVEC LES CONGRUENCES)

- Par 3 ou par 9 : la somme des chiffres est divisible par 3 (ou 9), car 10 ≡ 1 [9].
- Par 11 : la somme alternée des chiffres est divisible par 11, car 10 ≡ −1 [11].
- Par 4 : le nombre formé par les deux derniers chiffres est divisible par 4.

TABLEAU DE RESTES

Montrer que pour tout $n \in \mathbb{Z}$, $n^2 + 2$ n'est pas divisible par 4.

$n \equiv \ldots [4]$	0	1	2	3
$n^2 \equiv \ldots [4]$	0	1	0	1
$n^2 + 2 \equiv \ldots [4]$	2	3	2	3

Le reste n'est jamais 0 : $4 \nmid n^2 + 2$. ∎

PIÈGE

On ne peut **pas diviser** une congruence en général : $6 \equiv 2\ [4]$ mais $3 \not\equiv 1\ [4]$. Et on ne réduit pas un **exposant** modulo n : on cherche une puissance congrue à 1.

💡 بالعربية

$a \equiv b\ [n]$ (نقرأ: a **يوافق** b بترديد n) يعني أن n يقسم a - b، أي أن لهما نفس الباقي في القسمة على n. الموافقة **منسجمة** مع الجمع والضرب والقوى، وتمكن من حساب بواقي أعداد كبيرة جدا.

4 Nombres premiers

الأعداد الأولية

DÉFINITION — NOMBRE PREMIER

Un entier naturel p est **premier** s'il admet exactement **deux diviseurs positifs** : 1 et p. Ainsi 0 et 1 ne sont pas premiers. Les premiers nombres premiers sont :

2 ; 3 ; 5 ; 7 ; 11 ; 13 ; 17 ; 19 ; 23 ; 29 ; 31 ; 37 ; 41 ; 43 ; 47 ; ...

PROPRIÉTÉS

- Tout entier $n \geq 2$ admet au moins un diviseur premier.
- Si $n \geq 2$ n'est pas premier, il admet un diviseur premier p tel que $p^2 \leq n$, c'est-à-dire $p \leq \sqrt{n}$.
- **Il existe une infinité de nombres premiers** (Euclide).
- Si un nombre premier p divise un produit ab, alors $p \mid a$ ou $p \mid b$.

TEST DE PRIMALITÉ

Pour savoir si n est premier, on teste sa divisibilité par tous les nombres premiers $p \leq \sqrt{n}$. Si aucun ne divise n, alors n est premier.

EXEMPLES

391 : $\sqrt{391} \approx 19{,}8$. On teste 2, 3, 5, 7, 11, 13, 17 : $391 = 17 \times 23$. Non premier.

401 : $\sqrt{401} \approx 20{,}02$. Ni 2, 3, 5, 7, 11, 13, 17, 19 ne divisent 401. Donc **401 est premier**.

DÉMONSTRATION : IL EXISTE UNE INFINITÉ DE NOMBRES PREMIERS

Supposons qu'il n'y en ait qu'un nombre fini : $p_1, p_2, \ldots, p_k$. Posons $N = p_1 \times p_2 \times \ldots \times p_k + 1 \geq 2$. N a un diviseur premier, qui est l'un des p_i. Mais p_i divise le produit, donc il divise $N - p_1 \ldots p_k = 1$: impossible. ∎

DÉCOMPOSITION EN FACTEURS PREMIERS

Tout entier $n \geq 2$ s'écrit de façon **unique** (à l'ordre près) :

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

où les p_i sont des nombres premiers distincts et les $\alpha_i \in \mathbb{N}^*$.

NOMBRE DE DIVISEURS

Les diviseurs positifs de n sont les nombres $p_1^{\beta_1} \times \ldots \times p_k^{\beta_k}$ avec $0 \leq \beta_i \leq \alpha_i$. Leur nombre est :

$$(\alpha_1 + 1)(\alpha_2 + 1) \ldots (\alpha_k + 1)$$

EXEMPLE

$360 = 2^3 \times 3^2 \times 5$. Nombre de diviseurs positifs : $4 \times 3 \times 2 = 24$. 360 n'est pas un carré parfait (un exposant est impair) ; le plus petit entier m tel que 360m soit un carré est $m = 2 \times 5 = 10$ ($3600 = 60^2$).

PIÈGE

1 n'est **pas** premier, et 2 est le **seul** nombre premier pair. Pour un test de primalité, on s'arrête à $\sqrt{n}$: inutile d'aller plus loin.

بالعربية

العدد **الأولي** له قاسمان موجبان فقط: 1 ونفسه. لمعرفة هل n أولي نختبر قسمته على الأعداد الأولية p التي تحقق $p \leq \sqrt{n}$. كل عدد $n \geq 2$ يكتب بكيفية **وحيدة** كجداء عوامل أولية.

5 PGCD et PPCM

القاسم المشترك الأكبر والمضاعف المشترك الأصغر

DÉFINITION — PGCD ET PPCM

Soient a et b deux entiers naturels non nuls.

- Le **PGCD** de a et b, noté $a \wedge b$ ou PGCD(a ; b), est le plus grand diviseur commun à a et b.
- Le **PPCM**, noté $a \vee b$ ou PPCM(a ; b), est le plus petit multiple commun strictement positif de a et b.
- a et b sont **premiers entre eux** si $a \wedge b = 1$.

CALCUL AVEC LA DÉCOMPOSITION

- PGCD : produit des facteurs premiers **communs**, chacun avec le **plus petit** exposant.
- PPCM : produit de **tous** les facteurs premiers, chacun avec le **plus grand** exposant.

$$\text{PGCD}(a ; b) \times \text{PPCM}(a ; b) = a \times b$$

EXEMPLE

$2520 = 2^3 \times 3^2 \times 5 \times 7$ et $1960 = 2^3 \times 5 \times 7^2$.

PGCD $= 2^3 \times 5 \times 7 = 280$; PPCM $= 2^3 \times 3^2 \times 5 \times 7^2 = 17\,640$. Vérification :
$280 \times 17\,640 = 4\,939\,200 = 2520 \times 1960$ ✓.

ALGORITHME D'EUCLIDE

Si $a = bq + r$ (division euclidienne), alors PGCD(a ; b) = PGCD(b ; r). On répète les divisions : le PGCD est le **dernier reste non nul**.

EXEMPLE

PGCD(1071 ; 462) : $1071 = 462 \times 2 + 147$; $462 = 147 \times 3 + 21$; $147 = 21 \times 7 + 0$. Le dernier reste non nul est **21**.

PROPRIÉTÉS

- Les diviseurs communs à a et b sont exactement les diviseurs de PGCD(a ; b).
- Si d = PGCD(a ; b), alors a = da' et b = db' avec a' et b' **premiers entre eux**.
- PGCD(ka ; kb) = k × PGCD(a ; b) pour $k \in \mathbb{N}^*$.

PIÈGE

Ne pas confondre : PGCD → **plus petits** exposants des facteurs **communs** ; PPCM → **plus grands** exposants de **tous** les facteurs.

💡 **بالعربية**

القاسم المشترك الأكبر PGCD نحسبه بجداء العوامل الأولية **المشتركة** بأصغر أس، و**المضاعف المشترك الأصغر** PPCM بجداء **كل** العوامل بأكبر أس. PGCD × PPCM = a × b. **خوارزمية أقليدس**: PGCD هو آخر باق غير منعدم.

6 Exercices

تمارين — حاول أولاً قبل قراءة التصحيح!

10 exercices classés par difficulté. Les corrigés sont regroupés dans la partie suivante : cherche d'abord seul !

EXERCICE 1 — DIVISIBILITÉ APPLICATION

1. Déterminer les entiers relatifs n tels que $n - 2$ divise $3n + 1$.
2. Déterminer les entiers naturels n tels que $n + 1$ divise $n^2 + 5$.

EXERCICE 2 — DIVISION EUCLIDIENNE APPLICATION

1. Effectuer la division euclidienne de 2026 par 23, puis de -100 par 9.
2. Dans la division euclidienne d'un entier naturel a par 13, le quotient est égal au reste. Déterminer toutes les valeurs possibles de a.
3. Le reste de la division de a par 6 est 5. Quel est le reste de la division de a^2 par 6 ? de a par 3 ?

EXERCICE 3 — CONGRUENCES ET GRANDES PUISSANCES APPLICATION

1. Déterminer le reste de la division de 3^{100} par 7.
2. Déterminer le chiffre des unités de 2^{2026}.
3. Montrer que $5^{2n} - 1$ est divisible par 24 pour tout $n \in \mathbb{N}$.

EXERCICE 4 — NOMBRES PREMIERS APPLICATION

1. Les nombres 437, 499 et 1001 sont-ils premiers ?
2. Décomposer en produit de facteurs premiers : 1764 et 3780.
3. Combien 3780 a-t-il de diviseurs positifs ? 1764 est-il un carré parfait ?

EXERCICE 5 — PGCD ET PPCM APPLICATION

1. Calculer PGCD(3780 ; 1764) et PPCM(3780 ; 1764) à l'aide des décompositions.
2. Calculer PGCD(2026 ; 391) par l'algorithme d'Euclide.
3. Simplifier la fraction 1764/3780.

EXERCICE 6 — DISJONCTION DES CAS APPROFONDISSEMENT

1. Montrer que pour tout $n \in \mathbb{Z}$, $n^3 - n$ est divisible par 6.
2. Montrer que le carré d'un entier impair est congru à 1 modulo 8.
3. En déduire que l'équation $x^2 + y^2 = 4z + 3$ n'a pas de solution dans $\mathbb{Z}^3$.

EXERCICE 7 — PROBLÈME DE PGCD APPROFONDISSEMENT

1. Déterminer tous les couples (a ; b) d'entiers naturels tels que a + b = 84, a ≤ b et PGCD(a ; b) = 12.
2. Déterminer les couples (a ; b) d'entiers naturels tels que PGCD(a ; b) = 6 et PPCM(a ; b) = 90, avec a ≤ b.

EXERCICE 8 — CRITÈRE DE DIVISIBILITÉ PAR 11 APPROFONDISSEMENT

1. Montrer que $10 \equiv -1\ [11]$ et en déduire $10^k \equiv (-1)^k\ [11]$.
2. Soit $N = \overline{a_3a_2a_1a_0} = 1000a_3 + 100a_2 + 10a_1 + a_0$. Montrer que $11 \mid N \Leftrightarrow 11 \mid (a_0 - a_1 + a_2 - a_3)$.
3. 2794 et 7391 sont-ils divisibles par 11 ?

EXERCICE 9 — NOMBRES DE MERSENNE TYPE EXAMEN

1. Montrer que pour tous entiers $a \geq 1$ et $k \geq 1$: $2^a - 1$ divise $2^{ak} - 1$. (On pourra utiliser $2^a \equiv 1\ [2^a - 1]$.)
2. En déduire que si $2^n - 1$ est premier ($n \geq 2$), alors n est premier.
3. La réciproque est-elle vraie ? (Tester n = 11, sachant que 2047 = 23 × 89.)

EXERCICE 10 — SYNTHÈSE — TYPE EXAMEN TYPE EXAMEN

Soit $n \in \mathbb{N}$. On pose $a = n + 2$ et $b = 2n + 1$.

1. Montrer que PGCD(a ; b) divise 3.
2. Montrer que PGCD(a ; b) = 3 $\Leftrightarrow n \equiv 1\ [3]$.
3. Montrer que pour tout $n \in \mathbb{N}$: $7 \mid 3^{2n+1} + 2^{n+2}$.
4. Déterminer le reste de la division euclidienne de 3^{2026} par 13 (on calculera 3^3 modulo 13).

7 Corrigés détaillés

التصحيح المفصل للتمارين

CORRIGÉ 1 — DIVISIBILITÉ

1. $3n + 1 = 3(n - 2) + 7$. Donc
$n - 2 \mid 3n + 1 \Leftrightarrow n - 2 \mid 7 \Leftrightarrow n - 2 \in \{-7 ; -1 ; 1 ; 7\} \Leftrightarrow n \in \{-5 ; 1 ; 3 ; 9\}$.

2. $n^2 + 5 = (n + 1)(n - 1) + 6$. Donc $n + 1 \mid n^2 + 5 \Leftrightarrow n + 1 \mid 6$. Avec $n + 1 \geq 1$: $n + 1 \in \{1 ; 2 ; 3 ; 6\}$, soit $n \in \{0 ; 1 ; 2 ; 5\}$.

CORRIGÉ 2 — DIVISION EUCLIDIENNE

1. $2026 = 23 \times 88 + 2$; $-100 = 9 \times (-12) + 8$.

2. $a = 13q + q = 14q$ avec $0 \leq q < 13$: $a \in \{0 ; 14 ; 28 ; \ldots ; 168\}$ (13 valeurs).

3. $a = 6k + 5$: $a^2 = 36k^2 + 60k + 25 = 6(6k^2 + 10k + 4) + 1$, reste 1. $a = 3(2k + 1) + 2$: reste 2 dans la division par 3.

CORRIGÉ 3 — CONGRUENCES ET GRANDES PUISSANCES

1. $3^3 = 27 \equiv -1$ [7], donc $3^6 \equiv 1$ [7]. $100 = 6 \times 16 + 4$: $3^{100} \equiv 3^4 = 81 \equiv 4$ [7]. Reste 4.

2. $2^4 = 16 \equiv 6$ [10] et $6^k \equiv 6$ [10] pour $k \geq 1$. $2026 = 4 \times 506 + 2$:
$2^{2026} = (2^4)^{506} \times 4 \equiv 6 \times 4 = 24 \equiv 4$ [10]. Chiffre des unités : 4.

3. $5^2 = 25 \equiv 1$ [24], donc $5^{2n} = 25^n \equiv 1$ [24] et $24 \mid 5^{2n} - 1$. ∎

CORRIGÉ 4 — NOMBRES PREMIERS

1. $437 = 19 \times 23$: non premier. $\sqrt{499} \approx 22{,}3$: ni 2, 3, 5, 7, 11, 13, 17, 19 ne divisent 499 : **premier**.
$1001 = 7 \times 11 \times 13$: non premier.

2. $1764 = 2^2 \times 3^2 \times 7^2$; $3780 = 2^2 \times 3^3 \times 5 \times 7$.

3. $(2 + 1)(3 + 1)(1 + 1)(1 + 1) = 48$ diviseurs. $1764 = (2 \times 3 \times 7)^2 = 42^2$: oui, tous les exposants sont pairs.

CORRIGÉ 5 — PGCD ET PPCM

1. PGCD $= 2^2 \times 3^2 \times 7 = 252$; PPCM $= 2^2 \times 3^3 \times 5 \times 7^2 = 26\,460$. (Vérification :
$252 \times 26\,460 = 6\,667\,920 = 3780 \times 1764$.)

2. $2026 = 391 \times 5 + 71$; $391 = 71 \times 5 + 36$; $71 = 36 \times 1 + 35$; $36 = 35 \times 1 + 1$; $35 = 1 \times 35 + 0$.
PGCD = 1 : 2026 et 391 sont premiers entre eux.

3. On divise par le PGCD 252 : 1764/3780 = 7/15.

CORRIGÉ 6 — DISJONCTION DES CAS

1. $n^3 - n = (n-1)n(n+1)$: produit de trois entiers consécutifs. L'un d'eux est pair et l'un d'eux est multiple de 3, donc le produit est divisible par 2 et par 3, donc par 6 (2 et 3 étant premiers entre eux).

2. $n = 2k+1$: $n^2 = 4k^2 + 4k + 1 = 4k(k+1) + 1$, et $k(k+1)$ est pair, donc $4k(k+1)$ est multiple de 8 : $n^2 \equiv 1\ [8]$.

3. Modulo 4, un carré est congru à 0 (pair) ou 1 (impair). Donc $x^2 + y^2 \equiv 0, 1$ ou $2\ [4]$, jamais 3. Or $4z + 3 \equiv 3\ [4]$: pas de solution.

CORRIGÉ 7 — PROBLÈME DE PGCD

1. $a = 12a'$, $b = 12b'$ avec $\text{PGCD}(a' ; b') = 1$ et $a' + b' = 7$, $a' \leq b'$: $(1 ; 6)$, $(2 ; 5)$, $(3 ; 4)$ (tous premiers entre eux). Couples : $(12 ; 72)$, $(24 ; 60)$, $(36 ; 48)$.

2. $ab = 6 \times 90 = 540$; $a = 6a'$, $b = 6b'$ avec $a'b' = 15$, $a' \wedge b' = 1$, $a' \leq b'$: $(1 ; 15)$ ou $(3 ; 5)$. Couples : $(6 ; 90)$ et $(18 ; 30)$.

CORRIGÉ 8 — CRITÈRE DE DIVISIBILITÉ PAR 11

1. $10 - (-1) = 11$. En élevant à la puissance k : $10^k \equiv (-1)^k\ [11]$.

2. $N \equiv -a_3 + a_2 - a_1 + a_0\ [11]$, donc $N \equiv 0\ [11] \Leftrightarrow a_0 - a_1 + a_2 - a_3 \equiv 0\ [11]$. ∎

3. $2794 : 4 - 9 + 7 - 2 = 0$: oui ($2794 = 11 \times 254$). $7391 : 1 - 9 + 3 - 7 = -12$: non.

CORRIGÉ 9 — NOMBRES DE MERSENNE

1. $2^a \equiv 1\ [2^a - 1]$, donc $2^{ak} = (2^a)^k \equiv 1\ [2^a - 1] : 2^a - 1 \mid 2^{ak} - 1$. ∎

2. Contraposée : si n n'est pas premier, $n = ak$ avec $1 < a < n$. Alors $2^a - 1$ divise $2^n - 1$ avec $1 < 2^a - 1 < 2^n - 1 : 2^n - 1$ n'est pas premier. ∎

3. Non : 11 est premier mais $2^{11} - 1 = 2047 = 23 \times 89$ n'est pas premier.

CORRIGÉ 10 — SYNTHÈSE — TYPE EXAMEN

1. $d = \text{PGCD}(a ; b)$ divise a et b, donc divise $2a - b = 3$.

2. $d \in \{1 ; 3\}$. $d = 3 \Leftrightarrow 3 \mid a$ et $3 \mid b$. Or $3 \mid n + 2 \Leftrightarrow n \equiv 1\ [3]$, et dans ce cas $2n + 1 \equiv 3 \equiv 0\ [3]$. Donc $d = 3 \Leftrightarrow n \equiv 1\ [3]$.

3. $3^{2n+1} = 3 \times 9^n \equiv 3 \times 2^n\ [7]$ (car $9 \equiv 2\ [7]$) et $2^{n+2} = 4 \times 2^n$. Somme : $7 \times 2^n \equiv 0\ [7]$. ∎

4. $3^3 = 27 \equiv 1\ [13]$. $2026 = 3 \times 675 + 1 : 3^{2026} \equiv 3\ [13]$. Le reste est 3.

8 Fiche résumé

ملخص الدرس — للمراجعة السريعة

Quelle méthode pour quelle question ?

Je dois…	Méthode	بالعربية
trouver n tel que d(n) | N(n)	écrire N = q·d + constante, puis d | constante	قابلية القسمة
reste d'une grande puissance	trouver $a^k \equiv 1$ [n], puis division de l'exposant	الموافقة
divisibilité pour tout n	disjonction des cas (tableau de restes) ou récurrence	فصل الحالات
n est-il premier ?	tester les premiers $p \leq \sqrt{n}$	عدد أولي
PGCD, PPCM	décomposition (plus petits / plus grands exposants) ou Euclide	PGCD و PPCM
couples avec PGCD donné	a = da', b = db' avec a' ∧ b' = 1	أعداد أولية فيما بينها

L'ESSENTIEL

$$a \mid b \Leftrightarrow b = ka$$

$$a = bq + r,\ 0 \leq r < b$$

$$a \equiv b\ [n] \Leftrightarrow n \mid a - b$$

$$\text{nb de diviseurs} = \Pi\ (\alpha_i + 1)$$

$$\text{PGCD} \times \text{PPCM} = a \times b$$

TOP 5 DES ERREURS

- Donner un reste négatif ou ≥ b.
- Dire que 1 est premier.
- Diviser une congruence par un nombre.
- Réduire un exposant modulo n.
- Confondre les règles du PGCD et du PPCM.

Lexique français — arabe معجم المصطلحات

Français	العربية	Français	العربية
Diviseur	قاسم	Nombre premier	عدد أولي
Multiple	مضاعف	Décomposition	تفكيك
Divise	يقسم	Facteur premier	عامل أولي
Division euclidienne	القسمة الأقليدية	PGCD	القاسم المشترك الأكبر
Quotient	خارج	PPCM	المضاعف المشترك الأصغر
Reste	باقي	Premiers entre eux	أوليان فيما بينهما
Congru modulo n	يوافق بترديد n	Algorithme d'Euclide	خوارزمية أقليدس
Pair / impair	زوجي / فردي	Critère de divisibilité	معيار القسمة

Besoin d'aide sur ce chapitre ? Séance d'essai 100 % gratuite.

Cours en direct sur Google Meet · Petits groupes de 8 élèves max · Programme marocain · moraja3a.app · WhatsApp +212 617 638 536

احجز حصتك التجريبية المجانية على موقع moraja3a.app — افهم، تدرّب، انجح.