

Arithmétique — divisibilité et congruences

Terminale Maths expertes

Exercice 1 — Division euclidienne — quotient et reste

Pour $n \in \mathbb{N}$, on pose

$$A_n = 3n^2 + 8n + 5.$$

1. Montrer que $A_n = (n + 2)(3n + 2) + 1$.
2. Donner le quotient et le reste de la division euclidienne de A_n par $n + 2$.
3. Calculer $\text{PGCD}(A_n, n + 2)$.
4. En déduire que A_n et $n + 2$ sont premiers entre eux.

Exercice 2 — Premiers calculs de congruences

On travaille modulo 7.

1. Calculer les restes de $3, 3^2, 3^3, 3^4, 3^5, 3^6$ modulo 7.
2. Montrer que $3^6 \equiv 1 \pmod{7}$.
3. Déterminer le reste de 3^{2026} dans la division par 7.
4. Déterminer tous les entiers naturels n tels que $3^n \equiv -1 \pmod{7}$.

Exercice 3 — Algorithme d'Euclide

On considère les entiers 2520 et 1980.

1. Effectuer l'algorithme d'Euclide pour calculer leur PGCD.
2. Donner la suite des restes non nuls.
3. Remonter l'algorithme pour écrire le PGCD comme combinaison linéaire de 2520 et 1980.
4. En déduire des entiers u, v tels que $2520u + 1980v = 180$.

Exercice 4 — Bézout et inverse modulo 101

On travaille avec les entiers 101 et 37.

1. Calculer $\text{PGCD}(101, 37)$.
2. Déterminer des entiers u, v tels que $101u + 37v = 1$.
3. En déduire un inverse de 37 modulo 101.
4. Résoudre $37x \equiv 24 \pmod{101}$.

Exercice 5 — Décomposition en facteurs premiers et diviseurs

On considère l'entier

$$N = 45360.$$

1. Décomposer N en produit de facteurs premiers.
2. Déterminer le nombre de diviseurs positifs de N .
3. Déterminer le plus grand diviseur de N qui soit un carré parfait.
4. Déterminer le plus petit entier $k > 0$ tel que kN soit un carré parfait.

Exercice 6 — Divisibilité de $n^3 - n$ et $n^5 - n$

Soit $n \in \mathbb{Z}$.

1. Factoriser $n^3 - n$ et montrer que ce nombre est divisible par 6.

- Montrer, en étudiant les restes modulo 5, que $5 \mid n^5 - n$.
- Montrer que $2 \mid n^5 - n$ et $3 \mid n^5 - n$.
- En déduire que $\boxed{30 \mid n^5 - n}$ pour tout entier n .

Exercice 7 — Résoudre une congruence linéaire

On souhaite résoudre

$$14x \equiv 8 \pmod{30}.$$

- Calculer PGCD(14, 30) et expliquer pourquoi l'équation peut avoir des solutions.
- Réduire la congruence à une congruence modulo 15.
- Résoudre la congruence obtenue modulo 15.
- Donner toutes les solutions modulo 30.

Exercice 8 — Un PGCD égal à 1 pour tout n

Pour $n \in \mathbb{N}$, on pose

$$A = 6n + 5, \quad B = 4n + 3.$$

- Calculer $2A - 3B$.
- Montrer que A et B sont premiers entre eux.
- Montrer que 2 est un inverse de A modulo B .
- Si $A \mid Bk$, montrer que $A \mid k$.

Exercice 9 — Équation diophantienne — problème de billets

Des billets coûtent soit **23 €**, soit **17 €**. Une association dépense exactement **800 €**. On note x et y les nombres de billets achetés de chaque type.

- Écrire l'équation diophantienne vérifiée par x et y .
- Résoudre cette équation dans $\mathbb{Z}^2$.
- Déterminer les solutions vérifiant $x > 0$ et $y > 0$.
- Pour chacune de ces solutions, donner le nombre total de billets.

Exercice 10 — Étudier la primalité de 1009

On veut déterminer si 1009 est premier.

- Expliquer pourquoi il suffit de tester les nombres premiers inférieurs ou égaux à $\sqrt{1009}$.
- Donner la liste des nombres premiers à tester.
- Effectuer les tests et conclure.
- En déduire que tout entier a avec $1 \leq a < 1009$ est premier avec 1009.

Exercice 11 — PGCD dépendant d'un entier

Pour $n \in \mathbb{N}$, on pose

$$d_n = \text{PGCD}(2n + 1, n + 3).$$

- Montrer que $d_n \mid 5$.
- En déduire les seules valeurs possibles de d_n .
- Déterminer les entiers n pour lesquels $d_n = 5$.
- Donner l'expression complète de d_n selon la classe de n modulo 5.

Exercice 12 — Bézout puis équation diophantienne

On considère l'équation

$$527x + 221y = 17, \quad (x, y) \in \mathbb{Z}^2.$$

1. Calculer PGCD(527, 221).
2. Trouver une relation de Bézout donnant 17.
3. En déduire une solution particulière de l'équation.
4. Déterminer toutes les solutions entières.

Exercice 13 — Équation diophantienne avec contrainte de positivité

On cherche des entiers strictement positifs x, y tels que

$$84x + 66y = 1800.$$

1. Justifier que l'équation possède des solutions entières.
2. La simplifier puis déterminer une solution particulière.
3. Déterminer toutes les solutions dans $\mathbb{Z}^2$.
4. Déterminer toutes les solutions avec $x > 0$ et $y > 0$.

Exercice 14 — Théorème de Gauss — démonstration et applications

Soient $a, b, c \in \mathbb{Z}$ avec PGCD(a, b) = 1.

1. À l'aide de Bézout, montrer que si $a \mid bc$, alors $a \mid c$.
2. En déduire que si $35 \mid 12n$, alors $35 \mid n$.
3. Résoudre $12n \equiv 0 \pmod{35}$.
4. Montrer que si p est premier et $p \mid x^2$, alors $p \mid x$.

Exercice 15 — Système de trois congruences

Résoudre dans $\mathbb{Z}$

$$\begin{cases} x \equiv 2 \pmod{5}, \\ x \equiv 3 \pmod{7}, \\ x \equiv 4 \pmod{9}. \end{cases}$$

1. Résoudre d'abord les deux premières congruences.
2. Montrer qu'elles équivalent à $x \equiv 17 \pmod{35}$.
3. Introduire $x = 17 + 35t$ et utiliser la troisième congruence.
4. Donner toutes les solutions modulo 315.

Exercice 16 — Deux derniers chiffres d'une grande puissance

On cherche les deux derniers chiffres de

$$3^{2026}.$$

1. Calculer 3^{10} modulo 100.
2. En déduire que $3^{20} \equiv 1 \pmod{100}$.
3. Réduire l'exposant 2026 modulo 20.
4. Déterminer les deux derniers chiffres de 3^{2026} .

Exercice 17 — Petit théorème de Fermat et inverse

On travaille modulo le nombre premier 29.

1. Énoncer le petit théorème de Fermat et l'appliquer à 5.
2. Calculer 5^{2026} modulo 29.
3. Déterminer un inverse de 12 modulo 29.
4. Résoudre $12x \equiv 7 \pmod{29}$.

Exercice 18 — Carré d'un nombre premier supérieur à 3

Soit $p > 3$ un nombre premier.

1. Montrer que p est impair et que $p^2 \equiv 1 \pmod{8}$.
2. Montrer que $p^2 \equiv 1 \pmod{3}$.
3. En déduire que $p^2 \equiv 1 \pmod{24}$.
4. Montrer alors que $24 \mid (p-1)(p+1)$.

Exercice 19 — Répunités $11 \dots 1$ et divisibilité par 37

Pour $n \geq 1$, on pose

$$R_n = \frac{10^n - 1}{9}.$$

Ainsi R_n est l'entier formé de n chiffres 1.

1. Montrer que si $d \mid n$, alors $R_d \mid R_n$.
2. Vérifier que $37 \mid R_3$.
3. Montrer que $37 \mid R_n \iff 10^n \equiv 1 \pmod{37}$.
4. Déterminer tous les $n \geq 1$ tels que $37 \mid R_n$.

Exercice 20 — Facteurs premiers, diviseurs et carré parfait

On considère

$$N = 75600.$$

1. Décomposer N en facteurs premiers.
2. Calculer le nombre de diviseurs positifs de N .
3. Déterminer le plus grand carré parfait qui divise N .
4. Déterminer le plus petit entier $m \geq 1$ tel que mN soit un carré parfait.

Exercice 21 — Résoudre $x^2 \equiv 1 \pmod{35}$

On cherche les solutions de

$$x^2 \equiv 1 \pmod{35}.$$

1. Montrer que la congruence équivaut à $35 \mid (x-1)(x+1)$.
2. Résoudre séparément $x^2 \equiv 1 \pmod{5}$ et $x^2 \equiv 1 \pmod{7}$.
3. Combiner les possibilités et déterminer toutes les solutions modulo 35.
4. Comparer avec le cas d'un module premier p et expliquer pourquoi il n'y a alors que deux solutions.

Exercice 22 — Système de congruences à modules non premiers entre eux

Résoudre

$$\begin{cases} x \equiv 5 \pmod{12}, \\ x \equiv 11 \pmod{18}. \end{cases}$$

1. Calculer PGCD(12, 18) et vérifier la compatibilité des deux congruences.
2. Poser $x = 5 + 12k$ et obtenir une congruence en k .

3. Résoudre cette congruence puis déterminer x .
4. Expliquer pourquoi le système $x \equiv 4 \pmod{12}$, $x \equiv 11 \pmod{18}$ n'aurait aucune solution.

Exercice 23 — Chiffrement affine modulo 26

On code les lettres par $A = 0, B = 1, \dots, Z = 25$ et on chiffre par

$$E(x) \equiv 5x + 8 \pmod{26}.$$

1. Montrer que 5 est inversible modulo 26 et déterminer son inverse.
2. Établir une formule de déchiffrement $D(y)$.
3. Coder le mot MATHS.
4. Déchiffrer le mot obtenu et vérifier que l'on retrouve MATHS.

Exercice 24 — Nombres de Fermat et infinité des nombres premiers

Pour $n \in \mathbb{N}$, on définit

$$F_n = 2^{2^n} + 1.$$

1. Calculer F_0, F_1, F_2, F_3 .
2. Montrer par récurrence que $F_0 F_1 \cdots F_{n-1} = F_n - 2$ pour $n \geq 1$.
3. Montrer que deux nombres de Fermat distincts sont premiers entre eux.
4. En déduire qu'il existe une infinité de nombres premiers.

Exercice 25 — Nombres de Mersenne — condition nécessaire

Pour $n \geq 2$, on pose

$$M_n = 2^n - 1.$$

1. Supposer $n = ab$ avec $a, b > 1$ et factoriser M_n .
2. Montrer que si M_n est premier, alors n est premier.
3. Calculer M_{11} .
4. Vérifier que $M_{11} = 23 \times 89$ et expliquer pourquoi la réciproque de la question 2 est fausse.

Exercice 26 — PGCD de deux nombres de la forme $2^n - 1$

On pose

$$A = 2^{84} - 1, \quad B = 2^{30} - 1.$$

On cherche $\text{PGCD}(A, B)$ sans calculer A et B .

1. À partir de $84 = 2 \times 30 + 24$, montrer que $\text{PGCD}(A, B) = \text{PGCD}(2^{24} - 1, 2^{30} - 1)$.
2. Utiliser $30 = 24 + 6$ pour réduire encore le PGCD.
3. Montrer que $2^6 - 1$ divise $2^{24} - 1$.
4. En déduire $\text{PGCD}(A, B)$ et le décomposer en facteurs premiers.

Exercice 27 — Puissances modulo 13 — problème de synthèse

On étudie la divisibilité de

$$2^n + 3^n$$

par 13.

1. Montrer que $2^6 \equiv -1 \pmod{13}$ et $3^3 \equiv 1 \pmod{13}$.
2. En déduire que $13 \mid 2^{74} + 3^{74}$.
3. Déterminer l'inverse de 3 modulo 13 et montrer que $2^n + 3^n \equiv 0 \pmod{13} \iff 5^n \equiv -1 \pmod{13}$.

4. Déterminer tous les entiers $n \geq 1$ tels que $13 \mid 2^n + 3^n$.

Exercice 28 — Diviseurs premiers de $n^2 + n + 1$

Soit $n \in \mathbb{Z}$ et soit $p \neq 3$ un nombre premier tel que

$$p \mid n^2 + n + 1.$$

1. Utiliser $n^3 - 1 = (n - 1)(n^2 + n + 1)$ pour montrer que $n^3 \equiv 1 \pmod{p}$.
2. Montrer que $n \not\equiv 1 \pmod{p}$ et que $p \nmid n$.
3. À l'aide du petit théorème de Fermat, montrer que $3 \mid p - 1$.
4. En déduire que tout diviseur premier $p \neq 3$ de $n^2 + n + 1$ vérifie $p \equiv 1 \pmod{3}$, puis vérifier sur $n = 10$.

Exercice 29 — Système de congruences — construction à la Bézout

On cherche les entiers n tels que

$$\begin{cases} n \equiv 7 \pmod{17}, \\ n \equiv 11 \pmod{23}. \end{cases}$$

1. Trouver des entiers u, v tels que $17u + 23v = 1$.
2. Construire une solution $N = 7 \times 23v + 11 \times 17u$ et vérifier qu'elle convient.
3. Réduire N modulo 17×23 et déterminer toutes les solutions.
4. Déterminer le plus petit entier naturel solution.

Exercice 30 — Synthèse — chiffrement par puissance modulo un nombre premier

Les messages sont représentés par des entiers $m \in \{0, 1, \dots, 28\}$. On définit le chiffrement

$$E(m) \equiv m^5 \pmod{29}.$$

1. Montrer que 5 est premier avec 28 et déterminer d tel que $5d \equiv 1 \pmod{28}$.
2. À l'aide du petit théorème de Fermat, montrer que $(m^5)^d \equiv m \pmod{29}$ pour tout message m .
3. Chiffrer le message $m = 8$.
4. Déchiffrer le résultat obtenu en calculant $c^d \pmod{29}$.