

TD

Arithmétique

EXERCICES D'APPLICATION DU COURS

EXERCICE 1 ■ □ □

Montrer que $2026^{2025} - 1$ est un multiple de 3. ▶ Indication ▶ Correction

EXERCICE 2 ■ □ □

Donner le chiffre des unités de 2025^{2026} . ▶ Indication ▶ Correction

EXERCICE 3 ■ □ □

Déterminer le pgcd et les coefficients de l'égalité de Bézout des entiers a et b suivants

- ① $a = 33$ et $b = 24$, ② $a = 37$ et $b = 27$, ③ $a = 270$ et $b = 105$.

▶ Indication ▶ Correction

EXERCICE 4 ■ □ □

Trouver les chiffres a tel que le nombre d'écriture décimale $123a4$ soit divisible par 12.

▶ Indication ▶ Correction

EXERCICE 5 ■ ■ □

Déterminer un critère simple de parité pour un entier donné par son écriture en base 3.

▶ Indication ▶ Correction

EXERCICE 6 ■ □ □

Montrer que $10a + b$ avec $b \in \llbracket 0, 9 \rrbracket$ est divisible par 7 si, et seulement si, $a - 2b$ est divisible par 7. ▶ Indication ▶ Correction

EXERCICE 7 ■ ■ □

Montrer que, pour tout $n \in \mathbb{N}$, les fractions $\frac{15n+4}{10n+3}$, $\frac{21n+4}{14n+3}$ sont irréductibles.

▶ Indication ▶ Correction

EXERCICE 8 ■ ■ □ Une Application de Fermat

Considérons 2026 entiers tels que leur somme soit nulle.

Montrer que la somme de leurs puissances 37ièmes est divisible par 37. ▶ Indication

▶ Correction

EXERCICES TECHNIQUES

EXERCICE 9 ■ ■ □ A la main

Résoudre dans $\mathbb{Z}^2$ les équations suivantes

- ① $xy = 3x + 2y$ ② $\frac{1}{x} + \frac{1}{y} = \frac{1}{5}$ ③ $x^2 - y^2 - 4x - 2y = 5$

▶ Indication ▶ Correction

EXERCICE 10 ■ □ □

Montrer que pour tout $n \in \mathbb{N}^*$, on a

- ① $(2n+4) \wedge (3n+3) \in \{1, 2, 3, 6\}$ ③ $(3n^2+2n) \wedge (n+1) = 1$
 ② $(n^2+n) \wedge (2n+1) = 1$ ④ $(15n^2+8n+6) \wedge (30n^2+21n+13) = 1$

▶ Indication ▶ Correction

EXERCICE 11 ■ ■ □ Système pgcd/ppcm

Soient $(x, y) \in \mathbb{N}^2$.

- ① Résoudre le système $\begin{cases} x \wedge y = 18 \\ x \vee y = 540 \end{cases}$.
 ② Trouver une condition nécessaire et suffisante sur d et m pour qu'il existe $(x, y) \in \mathbb{N}^2$ tels que $x \wedge y = d$ et $x \vee y = m$.

▶ Indication ▶ Correction

EXERCICE 12 ■ ■ □

Soient $a, b \in \mathbb{Z}$.

- ① On suppose $a \wedge b = 1$. Montrer que $(a+b) \wedge ab = 1$.
 ② On revient au cas général. Calculer $\text{pgcd}(a+b, \text{ppcm}(a, b))$.

▶ Indication ▶ Correction

EXERCICE 13 ■ ■ □

Soit $n \geq 2$. Calculer (1) $n \vee (2n + 1)$, (2) $(n - 1) \vee (2n + 1)$.

► Indication ► Correction

EXERCICE 14 ■ ■ □

Soit a et b deux entiers relatifs non nuls et p un nombre premier.

- (1) Montrer que $v_p(a + b) \geq \min(v_p(a), v_p(b))$.
- (2) Trouver a, b et p tels que $v_p(a + b) > \min(v_p(a), v_p(b))$.
- (3) Montrer que si $v_p(a) \neq v_p(b)$, alors $v_p(a + b) = \min(v_p(a), v_p(b))$.

► Indication ► Correction

EXERCICE 15 ■ ■ ■

Soit $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$. Montrer que

$$\left\lfloor \frac{a}{b} \right\rfloor + \left\lfloor \frac{a+1}{b} \right\rfloor + \cdots + \left\lfloor \frac{a+b-1}{b} \right\rfloor = a.$$

► Indication ► Correction

EXERCICE 16 ■ ■ ■

Pour tout $n \in \mathbb{N}$, on pose $F_n = 2^{2^n} + 1$.

- (1) Montrer que pour tout $n \in \mathbb{N}^*$, $F_n = 2 + \prod_{k=0}^{n-1} F_k$.
- (2) Montrer que, si $n \neq m$, alors F_n et F_m sont premiers entre eux.

► Indication ► Correction

EXERCICE 17 ■ ■ □

- (1) Soit a et b deux entiers naturels non nuls. Montrer que $(a + b) \wedge (a \vee b) = a \wedge b$.

- (2) Trouver tous les couples $(a, b) \in (\mathbb{N}^*)^2$ tels que $\begin{cases} a + b = 144 \\ a \vee b = 420. \end{cases}$

► Indication ► Correction

EXERCICE 18 ■ □ □ **On refait le cours**

Soient $a, b, d \in \mathbb{Z}$. Montrer l'équivalence $(\exists u, v \in \mathbb{Z}, au + bv = d) \iff a \wedge b \mid d$.

► Indication ► Correction

EXERCICE 19 ■ ■ □

Trouver tous les couples d'entiers $(x, y) \in \mathbb{N}^2$ tels que $x \vee y + 11(x \wedge y) = 203$.

► Indication ► Correction

EXERCICE 20 ■ ■ □

Déterminer les solutions entières $(x, y) \in \mathbb{N}^2$ de l'équation $x \wedge y + x \vee y = y + 4$.

► Indication ► Correction

EXERCICE 21 ■ ■ □

Résoudre les systèmes d'équations suivants, d'inconnue $x \in \mathbb{Z}$

$$(1) \begin{cases} x \equiv 1[2] \\ x \equiv 2[3] \\ x \equiv 3[5] \end{cases} \quad (2) \begin{cases} x \equiv 1[6] \\ x \equiv 4[10] \\ x \equiv 7[15] \end{cases} \quad (3) \begin{cases} x \equiv 7[18] \\ x \equiv 1[30] \\ x \equiv 16[45] \end{cases}$$

► Indication ► Correction

EXERCICES "COMME EN COLLE"

EXERCICE 22 ■ □ □

Soit $(a, b, c) \in (\mathbb{N}^*)^3$ tel que $a^2 + b^2 = c^2$ et $a \wedge b \wedge c = 1$.

Montrer que $a \wedge b = a \wedge c = b \wedge c = 1$. ► Indication ► Correction

EXERCICE 23 ■ □ □

Soit $(a, b, c) \in (\mathbb{N}^*)^3$ tel que $a^2 + b^2 = c^2$ et $a \wedge b = 1$.

Montrer que a et b ne sont pas de même parité.

► Indication ► Correction

EXERCICE 24 ■ ■ □

① Déterminer les solutions entières (x, y) de l'équation $323x - 391y = 612$.

② Trouver tous les entiers n tels que $n = 270[323]$ et $n = 100[391]$.

► Indication ► Correction

EXERCICE 25 ■ ■ □

Pour $n \in \mathbb{N}^*$, on désigne par N le nombre de diviseurs positifs de n et par P leur produit. Quelle relation existe-t-il entre n, N et P ? ► Indication ► Correction

EXERCICE 26 ■ ■ □

Soient $a, m, n \in \mathbb{N}^*$ avec $a \geq 2$ et $m \leq n$. On note $d = (a^n - 1) \wedge (a^m - 1)$ et r le reste dans la division euclidienne de n par m .

① Montrer que $a^n \equiv a^r [a^m - 1]$.

② En déduire que $d = (a^r - 1) \wedge (a^m - 1)$, puis que $d = a^{n \wedge m} - 1$.

③ A quelle condition $a^m - 1 \mid a^n - 1$?

► Indication ► Correction

EXERCICE 27 ■ ■ □

Montrer que pour tout entier $n \geq 1$, $40^n n! \mid (5n)!$. ► Indication ► Correction

EXERCICE 28 ■ (A) ■ Nombres premiers de Fermat

Soient des entiers $a > 1$ et $n > 0$.

Montrer que si $a^n + 1$ est premier alors n est une puissance de 2.

► Indication ► Correction

EXERCICE 29 ■ ■ ■ Périodicité des restes

① Soit $n \geq 2$ et $a \in \mathbb{Z}$ un entier premier avec n .

Pour tout $k \in \mathbb{N}$, on note r_k le reste de la division euclidienne de a^k par n .

1.a) Montrer que $n \wedge r_k = 1$.

1.b) Dire pourquoi l'application $R : k \mapsto r_k$ n'est pas injective.

1.c) En déduire que la suite $(r_k)_{k \in \mathbb{N}}$ est périodique.

② Quel est le reste de la division euclidienne de 3^{2021} par 5 ?

► Indication ► Correction

EXERCICE 30 ■ ■ □ Nombres de Carmichael

Soit n un entier supérieur à 2. On suppose que n pour tout facteur premier p de n , p^2 ne divise pas n mais $p - 1$ divise $n - 1$.

Montrer que $\forall a \in \mathbb{Z}, a^n \equiv a [n]$. ► Indication ► Correction

EXERCICE 31 ■ ■ ■

① Montrer que $v_2(1000!) = 994$.

② Montrer que $\forall x \in \mathbb{R}, \left\lfloor \frac{\lfloor px \rfloor}{p} \right\rfloor = \lfloor x \rfloor$.

③ Plus généralement, calculer $v_p(n!)$.

► Indication ► Correction

EXERCICE 32 ■ □ □

① Montrer qu'un diviseur premier impair d'un entier de la forme $a^2 + 1$ avec $a \in \mathbb{Z}$ est congru à 1 modulo 4.

② En déduire que l'ensemble des nombres premiers congrus à 1 modulo 4 est infini.

► Indication ► Correction

Indications

EXERCICES D'APPLICATION DU COURS

INDICATION POUR L'EXERCICE 1

Un petit critère de divisibilité ?

[↩ retour à l'EXERCICE 1](#)

INDICATION POUR L'EXERCICE 2

Un petit critère de divisibilité ?

[↩ retour à l'EXERCICE 2](#)

INDICATION POUR L'EXERCICE 3

Algorithme d'Euclide étendu.

[↩ retour à l'EXERCICE 3](#)

INDICATION POUR L'EXERCICE 4

Critères de divisibilité par 3 et 4.

[↩ retour à l'EXERCICE 4](#)

INDICATION POUR L'EXERCICE 5

Ecrire en base 3 le nombre, puis faire la même preuve que pour les critères de divisibilité en base 10.

[↩ retour à l'EXERCICE 5](#)

INDICATION POUR L'EXERCICE 6

On multiplie par -2 dans la relation de congruence pour faire apparaître $-2b$, en justifiant pourquoi cela ne change pas la congruence.

[↩ retour à l'EXERCICE 6](#)

INDICATION POUR L'EXERCICE 7

Il suffit de montrer que, pour chaque fraction, le numérateur et le dénominateur sont premiers entre eux.

[↩ retour à l'EXERCICE 7](#)

INDICATION POUR L'EXERCICE 8 **Une Application de Fermat**

Théorème de Fermat.

[↩ retour à l'EXERCICE 8](#)

EXERCICES TECHNIQUES

INDICATION POUR L'EXERCICE 9 **A la main**

On essaie de factoriser pour exprimer les équations sous forme de produits de diviseurs d'un nombre.

[↩ retour à l'EXERCICE 9](#)

INDICATION POUR L'EXERCICE 10

Soit par division euclidienne, soit par conservation du pgcd par soustraction, on réduit la taille des nombres présents.

Pour les produits, on utilise " $a \wedge b = 1$ et $a \wedge c$, alors $a \wedge bc$ ".

[↩ retour à l'EXERCICE 10](#)

INDICATION POUR L'EXERCICE 11 **Système pgcd/ppcm**

On utilise la relation $d = a \wedge b \iff \begin{cases} \exists a' \in \mathbb{Z}, a = da' \\ \exists b' \in \mathbb{Z}, b = db' \\ a' \wedge b' = 1 \end{cases}$

[↩ retour à l'EXERCICE 11](#)

INDICATION POUR L'EXERCICE 12

① On utilise la stabilité du pgcd par somme et produit.

- ② On utilise la relation $d = a \wedge b \iff \begin{cases} \exists a' \in \mathbb{Z}, a = da' \\ \exists b' \in \mathbb{Z}, b = db' \\ a' \wedge b' = 1 \end{cases}$

[↩ retour à l'EXERCICE 12](#)

INDICATION POUR L'EXERCICE 13

On calcule le pgcd et on utilise la relation pgcd-ppcm.
S'il y a plusieurs pgcd possibles, on fait une disjonction de cas.

[↩ retour à l'EXERCICE 13](#)

INDICATION POUR L'EXERCICE 14

Utiliser la décomposition en facteurs premiers de a et b qui fait apparaître p .
Pour éviter les disjonctions de cas, on pourra supposer que $v_p(a) \leq v_p(b)$.

[↩ retour à l'EXERCICE 14](#)

INDICATION POUR L'EXERCICE 15

On déterminera les entiers $n \in \llbracket 0, b-1 \rrbracket$ tels que $\lfloor \frac{a+n}{b} \rfloor = \lfloor \frac{a}{b} \rfloor$ ainsi que ceux tels que $\lfloor \frac{a+n}{b} \rfloor = \lfloor \frac{a}{b} \rfloor + 1$.

On peut écrire la division euclidienne de a par b pour cela.

[↩ retour à l'EXERCICE 15](#)

INDICATION POUR L'EXERCICE 16

- ① Par récurrence.

- ② Pour $n < m$, montrer que $F_n \wedge F_m$ divise $\prod_{k=0}^{n-1} F_k$, puis 2. Conclure.

[↩ retour à l'EXERCICE 16](#)

INDICATION POUR L'EXERCICE 17

On utilise la relation $d = a \wedge b \iff \begin{cases} \exists a' \in \mathbb{Z}, a = da' \\ \exists b' \in \mathbb{Z}, b = db' \\ a' \wedge b' = 1 \end{cases}$

[↩ retour à l'EXERCICE 17](#)

INDICATION POUR L'EXERCICE 18 On refait le cours

Utiliser la particularité du pgcd par rapport aux autres diviseurs commun. Penser à l'égalité de Bézout.

[↩ retour à l'EXERCICE 18](#)

INDICATION POUR L'EXERCICE 19

On utilise la relation $d = a \wedge b \iff \begin{cases} \exists a' \in \mathbb{Z}, a = da' \\ \exists b' \in \mathbb{Z}, b = db' \\ a' \wedge b' = 1 \end{cases}$

[↩ retour à l'EXERCICE 19](#)

INDICATION POUR L'EXERCICE 20

On utilise la relation $d = a \wedge b \iff \begin{cases} \exists a' \in \mathbb{Z}, a = da' \\ \exists b' \in \mathbb{Z}, b = db' \\ a' \wedge b' = 1 \end{cases}$

[↩ retour à l'EXERCICE 20](#)

INDICATION POUR L'EXERCICE 21

Algorithme d'euclide étendu ou on force, au choix.

[↩ retour à l'EXERCICE 21](#)

EXERCICES "COMME EN COLLE"

INDICATION POUR L'EXERCICE 22

Par l'absurde, prendre un diviseur premier commun à deux des nombres et montrer qu'il ne peut valoir que 1.

[↩ retour à l'EXERCICE 22](#)

INDICATION POUR L'EXERCICE 23

Par l'absurde. On pourra utiliser des congruences modulo 4.

[↩ retour à l'EXERCICE 23](#)

INDICATION POUR L'EXERCICE 24

Algorithme d'Euclide étendu. Chercher un lien entre les deux questions.

[↩ retour à l'EXERCICE 24](#)

INDICATION POUR L'EXERCICE 25

Associer judicieusement les diviseur dans P^2

[↩ retour à l'EXERCICE 25](#)

INDICATION POUR L'EXERCICE 26

- ① Calculer $a^n - a^r$.
- ② Il suffit de faire l'algorithme d'Euclide entre n et m .

[↩ retour à l'EXERCICE 26](#)

INDICATION POUR L'EXERCICE 27

Par récurrence.

[↩ retour à l'EXERCICE 27](#)

INDICATION POUR L'EXERCICE 28 Nombres premiers de Fermat

Poser $n = 2^k(2p + 1)$ et montrer que $p = 0$.
On pensera à factoriser avec $A^N - B^N$.

[↩ retour à l'EXERCICE 28](#)

INDICATION POUR L'EXERCICE 29 Périodicité des restes

- ① R n'étant pas injective, les restes se répètent à un moment. On peut alors poser une période comme étant la différence entre cette répétition. Vérifier ensuite que cette période fonctionne.
- ② On applique le résultat démontré.

[↩ retour à l'EXERCICE 29](#)

INDICATION POUR L'EXERCICE 30 Nombres de Carmichael

Ecrire n comme un produit de nombre premiers 2 à 2 distincts et faire une disjonction de cas sur le fait que ces nombres divisent tous a ou non.

[↩ retour à l'EXERCICE 30](#)

INDICATION POUR L'EXERCICE 31

Il faut décomposer les nombres selon le nombre premier choisi, donc en pairs et impairs pour la première question.

[↩ retour à l'EXERCICE 31](#)

INDICATION POUR L'EXERCICE 32

Par l'absurde (on pensera à éliminer le cas pair dans la première question).

[↩ retour à l'EXERCICE 32](#)

Corrections**EXERCICES D'APPLICATION DU COURS**