BURHAN

Arithmétique dans $\mathbb{Z}$: exercices, entraînement

2ème Année Baccalauréat · Sciences Mathématiques · Mathématiques

Version en ligne : burhan.ma/2bac/sciences-mathematiques/mathematiques/arithmetique-dans-z/exercices/entrainement

Chapitre	Palier	Exercices
Arithmétique dans $\mathbb{Z}$	Entraînement	8

Exercice 1

Carrés modulo 7

1.

Recopie et complète le tableau des restes de x^2 dans la division par 7, selon le reste r de l'entier x dans la division par 7.

r	0	1	2	3	4	5	6
reste de x^2	?	?	?	?	?	?	?

INDICE

Si $x \equiv r\ [7]$, alors $x^2 \equiv r^2\ [7]$. Il suffit donc de calculer les sept carrés r^2, puis de les réduire modulo 7.

CORRIGÉ

Soit $x \in \mathbb{Z}$ et r son reste dans la division euclidienne par 7. Alors $x \equiv r\ [7]$. Par compatibilité des congruences avec le produit, $x^2 \equiv r^2\ [7]$.

Il suffit donc de réduire r^2 modulo 7. Les carrés 0, 1 et 4 sont déjà des restes. Pour les autres : $9 = 7 + 2$, $16 = 14 + 2$, $25 = 21 + 4$ et $36 = 35 + 1$.

r	0	1	2	3	4	5	6
reste de x^2	0	1	4	2	2	4	1

Conclusion. Le carré d'un entier est congru à 0, 1, 2 ou 4 modulo 7, jamais à 3, 5 ou 6. De plus, $x^2 \equiv 0\ [7]$ seulement lorsque $r = 0$.

2.

Montre que, pour tout entier relatif n, l'entier $n^2 + 4$ n'est pas divisible par 7.

INDICE

Raisonne par l'absurde : si $7 \mid n^2 + 4$, à quoi serait congru n^2 modulo 7 ? Compare avec le tableau.

CORRIGÉ

Soit $n \in \mathbb{Z}$. Supposons par l'absurde que $7 \mid n^2 + 4$.

Alors $n^2 \equiv -4\ [7]$. Comme $-4 = -7 + 3$, on a $n^2 \equiv 3\ [7]$.

Or, d'après le tableau de la question 1, aucun carré n'est congru à 3 modulo 7 : c'est une contradiction.

Conclusion. Pour tout entier relatif n, l'entier $n^2 + 4$ n'est pas divisible par 7.

3.

Soient x et y deux entiers relatifs tels que $7 \mid x^2 + y^2$. Montre que $7 \mid x$ et $7 \mid y$.

INDICE

Les restes de x^2 et de y^2 sont pris dans $\{0, 1, 2, 4\}$. Dresse le tableau de leurs sommes modulo 7 et repère les cases nulles.

CORRIGÉ

Restes possibles. D'après la question 1, il existe s et t dans $\{0, 1, 2, 4\}$ tels que $x^2 \equiv s\ [7]$ et $y^2 \equiv t\ [7]$. Par compatibilité avec la somme, $x^2 + y^2 \equiv s + t\ [7]$.

Tableau des sommes. On réduit $s + t$ modulo 7 :

$s+t$	$t=0$	$t=1$	$t=2$	$t=4$
$s=0$	0	1	2	4
$s=1$	1	2	3	5
$s=2$	2	3	4	6
$s=4$	4	5	6	1

Seule case nulle. C'est $s = t = 0$. Comme $7 \mid x^2 + y^2$, on a $s + t \equiv 0\ [7]$, donc $x^2 \equiv 0\ [7]$ et $y^2 \equiv 0\ [7]$.

Conclusion. D'après la question 1, cela n'arrive que si $x \equiv 0\ [7]$ et $y \equiv 0\ [7]$: ainsi $7 \mid x$ et $7 \mid y$.

4.

Déduis-en que l'équation $x^2 + y^2 = 77$ n'a aucune solution dans $\mathbb{Z}^2$.

INDICE

Suppose qu'un couple (x, y) convient et applique la question 3. Écris ensuite $x = 7x'$ et $y = 7y'$, et remplace dans l'équation.

CORRIGÉ

Supposons par l'absurde qu'un couple $(x, y) \in \mathbb{Z}^2$ vérifie $x^2 + y^2 = 77$.

Comme $77 = 7 \times 11$, on a $7 \mid x^2 + y^2$. D'après la question 3, $7 \mid x$ et $7 \mid y$: il existe x' et y' dans $\mathbb{Z}$ tels que $x = 7x'$ et $y = 7y'$.

En remplaçant dans l'équation :

$$49(x'^2 + y'^2) = 77,$$

donc $49 \mid 77$. Or $77 = 49 \times 1 + 28$, avec un reste $28 \neq 0$: contradiction.

Conclusion. L'équation $x^2 + y^2 = 77$ n'a aucune solution dans $\mathbb{Z}^2$.

Exercice 2

Deux preuves pour une divisibilité par 11

Pour tout entier naturel n, on pose $u_n = 5^{2n+1} + 2 \times 3^{n+1}$.

1.

Calcule u_0, u_1 et u_2, puis vérifie que chacun est divisible par 11.

INDICE

Remplace n par 0, 1 et 2 dans les exposants $2n+1$ et $n+1$ avant de calculer les puissances.

CORRIGÉ

On remplace n par 0, 1 et 2 :

$$\begin{aligned} u_0 &= 5^1 + 2 \times 3^1 \\ &= 5 + 6 = 11, \\ u_1 &= 5^3 + 2 \times 3^2 \\ &= 125 + 18 = 143, \\ u_2 &= 5^5 + 2 \times 3^3 \\ &= 3125 + 54 = 3179. \end{aligned}$$

Or $11 = 11 \times 1$, $143 = 11 \times 13$ et $3179 = 11 \times 289$.

Conclusion. $u_0 = 11$, $u_1 = 143$ et $u_2 = 3179$ sont tous les trois divisibles par 11.

2.

Montre que $u_{n+1} = 25u_n - 44 \times 3^{n+1}$ pour tout entier naturel n. Démontre ensuite par récurrence que $11 \mid u_n$ pour tout $n \in \mathbb{N}$.

INDICE

Écris $5^{2n+3} = 25 \times 5^{2n+1}$, puis remplace 5^{2n+1} par $u_n - 2 \times 3^{n+1}$. Pour l'hérédité, remarque que $44 = 4 \times 11$.

CORRIGÉ

Relation de récurrence. Soit $n \in \mathbb{N}$. Par définition de u_n, on a $5^{2n+1} = u_n - 2 \times 3^{n+1}$. Donc :

$$\begin{aligned} u_{n+1} &= 5^{2n+3} + 2 \times 3^{n+2} \\ &= 25 \times 5^{2n+1} \\ &\quad + 6 \times 3^{n+1} \\ &= 25\left(u_n - 2 \times 3^{n+1}\right) \\ &\quad + 6 \times 3^{n+1} \\ &= 25u_n - 44 \times 3^{n+1}. \end{aligned}$$

Initialisation. $u_0 = 11$, donc $11 \mid u_0$.

Hérédité. Soit $n \in \mathbb{N}$ tel que $11 \mid u_n$: il existe $m \in \mathbb{Z}$ tel que $u_n = 11m$. Comme $44 = 4 \times 11$:

$$\begin{aligned} u_{n+1} &= 25 \times 11m \\ &\quad - 4 \times 11 \times 3^{n+1} \\ &= 11\left(25m - 4 \times 3^{n+1}\right). \end{aligned}$$

Comme $25m - 4 \times 3^{n+1}$ est un entier, $11 \mid u_{n+1}$.

Conclusion. Pour tout $n \in \mathbb{N}$, $u_{n+1} = 25u_n - 44 \times 3^{n+1}$. Par récurrence, $11 \mid u_n$ pour tout $n \in \mathbb{N}$.

3.

Démontre le même résultat sans récurrence, à l'aide des congruences modulo 11.

INDICE

Réduis d'abord 25 modulo 11. Écris ensuite $5^{2n+1} = 5 \times 25^n$ et $2 \times 3^{n+1} = 6 \times 3^n$.

CORRIGÉ

Soit $n \in \mathbb{N}$. On écrit $5^{2n+1} = 5 \times 25^n$ et $2 \times 3^{n+1} = 6 \times 3^n$, donc $u_n = 5 \times 25^n + 6 \times 3^n$.

Réduction de 25. On a $25 = 11 \times 2 + 3$, donc $25 \equiv 3\ [11]$. Par compatibilité avec les puissances, $25^n \equiv 3^n\ [11]$.

Calcul. Par compatibilité avec le produit et la somme :

$$\begin{aligned} u_n &\equiv 5 \times 3^n + 6 \times 3^n \\ &\equiv 11 \times 3^n \\ &\equiv 0\ [11]. \end{aligned}$$

Conclusion. Pour tout entier naturel n, $11 \mid u_n$.

4.

Montre que, pour tout entier naturel n, le reste de u_n dans la division euclidienne par 3 est 2.

INDICE

Modulo 3, le terme $2 \times 3^{n+1}$ disparaît. Réduis ensuite 5 et 25 modulo 3.

CORRIGÉ

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

Réductions. Comme $n + 1 \geq 1$, l'entier $2 \times 3^{n+1}$ est un multiple de 3 : $2 \times 3^{n+1} \equiv 0\ [3]$. De plus, $5 \equiv 2\ [3]$ et $25 = 3 \times 8 + 1$, donc $25 \equiv 1\ [3]$.

Calcul. Par compatibilité avec le produit, la somme et les puissances :

$$\begin{aligned} u_n &= 5 \times 25^n \\ &\quad + 2 \times 3^{n+1} \\ &\equiv 2 \times 1^n + 0 \\ &\equiv 2\ [3]. \end{aligned}$$

Conclusion. Comme $0 \leq 2 < 3$, le reste de u_n dans la division euclidienne par 3 est 2, pour tout entier naturel n.

Exercice 3

Quand le plus petit diviseur premier est grand

Soit n un entier naturel composé et p son plus petit diviseur premier. On pose $m = \dfrac{n}{p}$; c'est un entier naturel, car $p \mid n$.

1.

Montre que $m \geq 2$, puis que $m \geq p$.

INDICE

Pour $m \geq 2$, raisonne par l'absurde sur le cas $m = 1$. Pour la seconde inégalité, m est un diviseur de n au moins égal à 2 : compare-le au plus petit d'entre eux.

CORRIGÉ

Minoration $m \geq 2$. On a $n = pm$. Comme $n \geq 2$, l'entier naturel m est non nul. Supposons par l'absurde que $m = 1$. Alors $n = p$ serait premier, ce qui contredit l'hypothèse « n composé ». Donc $m \geq 2$.

Le plus petit diviseur de n. Notons k le plus petit diviseur de n au moins égal à 2. D'après la propriété du plus petit diviseur premier, k est premier, donc $k \geq p$. Inversement, p est un diviseur de n au moins égal à 2, donc $p \geq k$. Ainsi $k = p$.

Minoration $m \geq p$. L'entier m divise n et $m \geq 2$, donc $m \geq k = p$.

Conclusion. On a bien $m \geq 2$, puis $m \geq p$.

2.

On suppose dans cette question que m est composé, et on note p' le plus petit diviseur premier de m. Montre que $p' \geq p$, puis que $n \geq p^3$.

INDICE

Un diviseur de m est aussi un diviseur de n. Pour la seconde partie, un entier composé est au moins égal au carré de son plus petit diviseur premier.

CORRIGÉ

Comparaison de p' et p. On a $p' \mid m$ et $m \mid n$, donc $p' \mid n$ par transitivité. Ainsi p' est un diviseur premier de n. Comme p est le plus petit, $p' \geq p$.

Minoration de n. L'entier m est composé et p' est son plus petit diviseur premier, donc $p'^2 \leq m$. Comme $p' \geq p > 0$:

$$\begin{aligned} n = pm &\geq p \times p'^2 \\ &\geq p \times p^2 = p^3. \end{aligned}$$

Conclusion. Si m est composé, alors $p' \geq p$ et $n \geq p^3$.

3.

Déduis-en que, si $p^3 > n$, alors m est un nombre premier.

INDICE

Raisonne par l'absurde à partir de la question 2, sans oublier que $m \geq 2$.

CORRIGÉ

Supposons $p^3 > n$. D'après la question 1, $m \geq 2$: l'entier m est donc premier ou composé.

Supposons par l'absurde que m soit composé. La question 2 donne alors $n \geq p^3$, ce qui contredit $p^3 > n$.

Conclusion. Si $p^3 > n$, alors m est un nombre premier.

4.

Application : détermine le plus petit diviseur premier p de 323 et vérifie que $p^3 > 323$. Que peux-tu en conclure pour le quotient $\dfrac{323}{p}$?

INDICE

Teste les nombres premiers $2, 3, 5, 7, 11, 13, \ldots$ dans l'ordre, jusqu'au premier qui divise 323. Vérifie aussi que 323 est composé.

CORRIGÉ

Plus petit diviseur premier. On teste les nombres premiers dans l'ordre :

- $323 = 2 \times 161 + 1$;
- $323 = 3 \times 107 + 2$;
- $323 = 5 \times 64 + 3$;
- $323 = 7 \times 46 + 1$;
- $323 = 11 \times 29 + 4$;
- $323 = 13 \times 24 + 11$;
- $323 = 17 \times 19 + 0$.

Chaque reste est positif et strictement inférieur au diviseur : ce sont des divisions euclidiennes. Le plus petit diviseur premier de 323 est donc $p = 17$. De plus, 323 est composé, car $1 < 17 < 323$.

Application de la question 3. On a $17^3 = 4913 > 323$. D'après la question 3, le quotient

$$\frac{323}{17} = 19$$

est un nombre premier.

Conclusion. On a $p = 17$ et $p^3 > 323$, donc le quotient $\dfrac{323}{17} = 19$ est premier : $323 = 17 \times 19$.

Exercice 4

Le PGCD de 3n + 11 et n + 2

Pour tout entier naturel n, on pose $a = 3n + 11$ et $b = n + 2$.

1.

Montre que tout diviseur commun à a et b divise 5. Déduis-en que $a \wedge b$ vaut 1 ou 5.

INDICE

Cherche une combinaison $a - kb$, avec k entier, dans laquelle n disparaît. Un diviseur commun à deux entiers divise toute combinaison de ces entiers.

CORRIGÉ

Une combinaison sans n. On a $a - 3b = 3n + 11 - 3n - 6 = 5$.

Diviseurs communs. Soit $c \in \mathbb{Z}$ un diviseur commun à a et b. Il divise toute combinaison de a et de b, en particulier $a - 3b$. Donc $c \mid 5$.

Conclusion. En particulier, $a \wedge b$ est un diviseur positif de 5. Comme 5 est premier, $a \wedge b = 1$ ou $a \wedge b = 5$.

2.

Montre que $a \wedge b = 5$ si et seulement si $n \equiv 3\ [5]$.

INDICE

Si $a \wedge b = 5$, alors 5 divise $b = n + 2$. Pour la réciproque, calcule a et b modulo 5 lorsque $n \equiv 3\ [5]$.

CORRIGÉ

Sens direct. Supposons $a \wedge b = 5$. Alors $5 \mid b$, c'est-à-dire $n + 2 \equiv 0\ [5]$. Donc $n \equiv -2\ [5]$, soit $n \equiv 3\ [5]$.

Réciproque. Supposons $n \equiv 3\ [5]$. Alors $b = n + 2 \equiv 3 + 2 = 5 \equiv 0\ [5]$. De même, $a = 3n + 11 \equiv 9 + 11 = 20 \equiv 0\ [5]$.

Ainsi 5 est un diviseur commun positif de a et b, donc $5 \leq a \wedge b$. D'après la question 1, $a \wedge b = 5$.

Conclusion. $a \wedge b = 5$ si et seulement si $n \equiv 3\ [5]$.

3.

On suppose $n \equiv 3\ [5]$ et on écrit $n = 5k + 3$, avec $k \in \mathbb{N}$. Exprime a et b en fonction de k, puis montre que $3k + 4$ et $k + 1$ sont premiers entre eux.

INDICE

Factorise 5 dans a et dans b. Pour la primalité relative, cherche une combinaison de $3k + 4$ et de $k + 1$ égale à 1.

CORRIGÉ

Écriture de a et b. Avec $n = 5k + 3$:

$$\begin{aligned} a &= 3(5k + 3) + 11 \\ &= 15k + 20 \\ &= 5(3k + 4), \end{aligned}$$

$$b = 5k + 5 = 5(k + 1).$$

Primalité relative. On a $1 \times (3k + 4) - 3 \times (k + 1) = 1$. D'après le théorème de Bézout, $(3k + 4) \wedge (k + 1) = 1$.

Conclusion. $a = 5(3k + 4)$ et $b = 5(k + 1)$, et les entiers $3k + 4$ et $k + 1$ sont premiers entre eux.

4.

Toujours pour $n = 5k + 3$, exprime $a \vee b$ en fonction de k. Vérifie ta formule pour $n = 8$.

INDICE

Utilise la relation entre le produit ab, le PGCD et le PPCM de deux entiers naturels non nuls. Les écritures de la question 3 redonnent le PGCD.

CORRIGÉ

PGCD. D'après la question 3, $a = 5(3k + 4)$ et $b = 5(k + 1)$, avec $(3k + 4) \wedge (k + 1) = 1$. On retrouve ainsi $a \wedge b = 5$, car $a \wedge b = 5\,((3k + 4) \wedge (k + 1))$.

PPCM. Les entiers naturels a et b sont non nuls, donc $(a \wedge b)(a \vee b) = ab$:

$$\begin{aligned} a \vee b &= \frac{ab}{a \wedge b} \\ &= \frac{25(3k + 4)(k + 1)}{5} \\ &= 5(3k + 4)(k + 1). \end{aligned}$$

Vérification pour $n = 8$. On a $8 = 5 \times 1 + 3$, donc $k = 1$, $a = 35$ et $b = 10$. La formule donne $5 \times 7 \times 2 = 70$. Directement, 35 n'est pas multiple de 10, et $70 = 35 \times 2 = 10 \times 7$. Donc $35 \vee 10 = 70$.

Conclusion. Pour $n = 5k + 3$, $a \vee b = 5(3k + 4)(k + 1)$; pour $n = 8$, on trouve bien 70.

5.

Pour $n = 6$, justifie que $a \wedge b = 1$, puis trouve par l'algorithme d'Euclide un couple (u, v) d'entiers relatifs tel que $au + bv = 1$.

INDICE

Ici $a = 29$ et $b = 8$, et 6 n'est pas congru à 3 modulo 5. Écris les divisions successives, puis remonte-les en isolant chaque reste.

CORRIGÉ

PGCD. On a $6 = 5 \times 1 + 1$, donc $6 \equiv 1\ [5]$ et $6 \not\equiv 3\ [5]$. D'après les questions 1 et 2, $a \wedge b = 1$, avec $a = 29$ et $b = 8$.

Algorithme d'Euclide.

- $29 = 8 \times 3 + 5$;
- $8 = 5 \times 1 + 3$;
- $5 = 3 \times 1 + 2$;
- $3 = 2 \times 1 + 1$;
- $2 = 1 \times 2 + 0$.

Remontée. On isole chaque reste, à partir du dernier reste non nul :

$$\begin{aligned} 1 &= 3 - 2 \\ &= 3 - (5 - 3) \\ &= 2 \times 3 - 5 \\ &= 2 \times (8 - 5) - 5 \\ &= 2 \times 8 - 3 \times 5 \\ &= 2 \times 8 \\ &\quad - 3 \times (29 - 3 \times 8) \\ &= 11 \times 8 - 3 \times 29. \end{aligned}$$

Conclusion. Le couple $(u, v) = (-3, 11)$ convient : $29 \times (-3) + 8 \times 11 = -87 + 88 = 1$.

Exercice 5

250 dattes en boîtes de 13 et de 8

Une coopérative conditionne exactement 250 dattes dans des boîtes de 13 et des boîtes de 8, toutes pleines. On note x le nombre de boîtes de 13 et y celui des boîtes de 8. On étudie d'abord, dans $\mathbb{Z}^2$, l'équation (E) : $13x + 8y = 250$.

1.

Justifie que (E) admet des solutions dans $\mathbb{Z}^2$, puis vérifie que le couple $(2, 28)$ en est une.

INDICE

Calcule $13 \wedge 8$, par exemple avec l'algorithme d'Euclide, et regarde s'il divise le second membre.

CORRIGÉ

PGCD. Algorithme d'Euclide :

- $13 = 8 \times 1 + 5$;
- $8 = 5 \times 1 + 3$;
- $5 = 3 \times 1 + 2$;
- $3 = 2 \times 1 + 1$;
- $2 = 1 \times 2 + 0$.

Le dernier reste non nul est 1, donc $13 \wedge 8 = 1$.

Existence de solutions. Comme $13 \wedge 8 = 1$ et $1 \mid 250$, l'équation (E) admet des solutions dans $\mathbb{Z}^2$.

Une solution particulière. On a $13 \times 2 + 8 \times 28 = 26 + 224 = 250$.

Conclusion. L'équation (E) admet des solutions dans $\mathbb{Z}^2$, et le couple $(2, 28)$ en est une.

2.

Montre, à l'aide du théorème de Gauss, que les solutions de (E) dans $\mathbb{Z}^2$ sont les couples $(2+8k,\ 28-13k)$, avec $k \in \mathbb{Z}$.

INDICE

Soustrais membre à membre $13x+8y=250$ et $13\times 2+8\times 28=250$, puis regroupe pour obtenir $13(x-2)=8(28-y)$.

CORRIGÉ

Analyse. Soit $(x,y)\in\mathbb{Z}^2$ une solution de (E). On soustrait membre à membre l'égalité $13\times 2+8\times 28=250$:

$$13(x-2)=8(28-y).$$

Ainsi $8 \mid 13(x-2)$. Or $8\wedge 13=1$ (question 1). D'après le théorème de Gauss, $8 \mid x-2$: il existe $k\in\mathbb{Z}$ tel que $x=2+8k$.

En remplaçant, $13\times 8k=8(28-y)$. On simplifie par $8\neq 0$: $28-y=13k$, soit $y=28-13k$.

Synthèse. Soit $k\in\mathbb{Z}$. Alors :

$$\begin{aligned}&13(2+8k)+8(28-13k)\\&=26+104k\\&\quad+224-104k\\&=250.\end{aligned}$$

Conclusion. Les solutions de (E) dans $\mathbb{Z}^2$ sont exactement les couples $(2+8k,\ 28-13k)$, avec $k\in\mathbb{Z}$.

3.

Détermine toutes les façons de conditionner les 250 dattes.

INDICE

Ici, x et y sont des entiers naturels. Écris les deux inégalités $2+8k \geq 0$ et $28-13k \geq 0$, puis encadre l'entier k.

CORRIGÉ

Les nombres de boîtes x et y sont des entiers naturels. D'après la question 2, il existe $k \in \mathbb{Z}$ tel que $x = 2+8k$ et $y = 28-13k$. Il faut donc $2+8k \geq 0$ et $28-13k \geq 0$.

- $2+8k \geq 0$ donne $8k \geq -2$. Si $k \leq -1$, alors $8k \leq -8 < -2$. Donc $k \geq 0$.
- $28-13k \geq 0$ donne $13k \leq 28$. Si $k \geq 3$, alors $13k \geq 39 > 28$. Donc $k \leq 2$.

Ainsi $k \in \{0,1,2\}$. Réciproquement, chacune de ces valeurs convient :

k	x	y	**contrôle**
0	2	28	$26+224=250$
1	10	15	$130+120=250$
2	18	2	$234+16=250$

Conclusion. Il y a trois façons de conditionner les 250 dattes : 2 boîtes de 13 et 28 de 8 ; 10 boîtes de 13 et 15 de 8 ; 18 boîtes de 13 et 2 de 8.

4.

Quelle façon utilise le moins de boîtes ? Justifie.

INDICE

Exprime le nombre total de boîtes $x+y$ en fonction de k, puis regarde comment il varie quand k augmente.

CORRIGÉ

Soit $k \in \{0,1,2\}$. Le nombre total de boîtes est :

$$\begin{aligned} x+y &= (2+8k) \\ &\quad + (28-13k) \\ &= 30-5k. \end{aligned}$$

Il diminue quand k augmente : il vaut 30, 25 puis 20 pour $k = 0$, 1 puis 2.

Conclusion. La façon qui utilise le moins de boîtes correspond à $k = 2$: 20 boîtes, soit 18 boîtes de 13 et 2 boîtes de 8.

Exercice 6

Inverser 10 modulo 37

1.

Montre que $10 \wedge 37 = 1$ et trouve un couple (u, v) d'entiers relatifs tel que $10u + 37v = 1$.

INDICE

Applique l'algorithme d'Euclide à 37 et 10. Remonte ensuite les divisions à partir du dernier reste non nul, en isolant chaque reste.

CORRIGÉ

PGCD. Algorithme d'Euclide :

- $37 = 10 \times 3 + 7$;
- $10 = 7 \times 1 + 3$;
- $7 = 3 \times 2 + 1$;
- $3 = 1 \times 3 + 0$.

Le dernier reste non nul est 1 : $10 \wedge 37 = 1$.

Remontée. On isole chaque reste, à partir du dernier reste non nul :

$$\begin{aligned} 1 &= 7 - 2 \times 3 \\ &= 7 - 2 \times (10 - 7) \\ &= 3 \times 7 - 2 \times 10 \\ &= 3 \times (37 - 3 \times 10) \\ &\quad - 2 \times 10 \\ &= 3 \times 37 - 11 \times 10. \end{aligned}$$

Conclusion. $10 \wedge 37 = 1$, et le couple $(u, v) = (-11, 3)$ convient : $10 \times (-11) + 37 \times 3 = -110 + 111 = 1$.

2.

Déduis-en que $\overline{10}$ est inversible dans $\mathbb{Z}/37\mathbb{Z}$, et donne son inverse sous la forme $\overline{r}$, avec $0 \leq r \leq 36$.

INDICE

Lis l'égalité de la question 1 modulo 37 : le terme $37v$ disparaît. Ramène ensuite -11 entre 0 et 36.

CORRIGÉ

Inversibilité. D'après la question 1, $10 \times (-11) = 1 - 37 \times 3$. Donc $10 \times (-11) \equiv 1 \ [37]$, c'est-à-dire :

$$\overline{10} \times \overline{-11} = \overline{1}.$$

La classe $\overline{10}$ est donc inversible dans $\mathbb{Z}/37\mathbb{Z}$, d'inverse $\overline{-11}$.

Représentant entre 0 et 36. On a $-11 = 37 \times (-1) + 26$, avec $0 \leq 26 < 37$. Donc $\overline{-11} = \overline{26}$.

Conclusion. $\overline{10}$ est inversible dans $\mathbb{Z}/37\mathbb{Z}$, d'inverse $\overline{26}$. Contrôle : $10 \times 26 = 260$ et $260 = 37 \times 7 + 1$.

3.

Résous dans $\mathbb{Z}$ l'équation $10x \equiv 7\ [37]$.

INDICE

Multiplie les deux membres par 26. Le point délicat : justifie que l'équation obtenue est équivalente à la première, dans les deux sens.

CORRIGÉ

Analyse. Soit $x \in \mathbb{Z}$ tel que $10x \equiv 7\ [37]$. On multiplie les deux membres par 26 : $260x \equiv 182\ [37]$. Or $260 = 37 \times 7 + 1$, donc $260 \equiv 1\ [37]$. De plus, $182 = 37 \times 4 + 34$, avec $0 \leq 34 < 37$. Donc $x \equiv 34\ [37]$.

Synthèse. Soit $x \in \mathbb{Z}$ tel que $x \equiv 34\ [37]$. Alors $10x \equiv 340\ [37]$. Or $340 = 37 \times 9 + 7$, donc $10x \equiv 7\ [37]$.

Conclusion. Les solutions dans $\mathbb{Z}$ de $10x \equiv 7\ [37]$ sont les entiers $x = 34 + 37k$, avec $k \in \mathbb{Z}$.

4.

Montre que, dans $\mathbb{Z}/38\mathbb{Z}$, l'équation $\overline{10} \times x = \overline{7}$ n'a aucune solution. Quelle hypothèse a changé par rapport à la question 3 ?

INDICE

Calcule $10 \wedge 38$. Si une classe $\overline{c}$ convenait, quel entier diviserait à la fois 38 et $10c - 7$?

CORRIGÉ

PGCD. Algorithme d'Euclide : $38 = 10 \times 3 + 8$, $10 = 8 \times 1 + 2$ et $8 = 2 \times 4 + 0$. Le dernier reste non nul est 2, donc $10 \wedge 38 = 2$.

Absence de solution. Supposons par l'absurde qu'il existe $c \in \mathbb{Z}$ tel que $\overline{10} \times \overline{c} = \overline{7}$ dans $\mathbb{Z}/38\mathbb{Z}$. Alors $10c \equiv 7\ [38]$, donc $38 \mid 10c - 7$, puis $2 \mid 10c - 7$. Comme $2 \mid 10c$, l'entier 2 divise aussi la différence :

$$10c - (10c - 7) = 7.$$

C'est faux, car $7 = 2 \times 3 + 1$.

Conclusion. L'équation $\overline{10} \times x = \overline{7}$ n'a aucune solution dans $\mathbb{Z}/38\mathbb{Z}$. Ce qui a changé : 10 n'est plus premier avec le module, car $10 \wedge 38 = 2$. Donc $\overline{10}$ n'est pas inversible dans $\mathbb{Z}/38\mathbb{Z}$.

Exercice 7

42 divise $n^7 - n$

Soit n un entier relatif. On veut montrer que 42 divise $n^7 - n$, en remarquant que $42 = 2 \times 3 \times 7$.

1.

Montre que $7 \mid n^7 - n$.

INDICE

Utilise la forme du petit théorème de Fermat qui ne demande aucune hypothèse sur n. Il reste seulement à vérifier que 7 est premier.

CORRIGÉ

7 **est premier.** Le seul nombre premier p tel que $p^2 \leq 7$ est 2, et $7 = 2 \times 3 + 1$: 2 ne divise pas 7. Donc 7 est premier.

Petit théorème de Fermat. Pour tout nombre premier p et tout $n \in \mathbb{Z}$, $n^p \equiv n\ [p]$. Avec $p = 7$, on obtient $n^7 \equiv n\ [7]$.

Conclusion. $7 \mid n^7 - n$.

2.

Montre que $3 \mid n^7 - n$.

INDICE

Applique le petit théorème de Fermat avec $p = 3$, puis écris n^7 à l'aide de n^3.

CORRIGÉ

3 **est premier** : ses seuls diviseurs positifs sont 1 et 3. D'après le petit théorème de Fermat, $n^3 \equiv n\ [3]$.

Réduction de n^7. Par compatibilité des congruences avec le produit :

$$\begin{aligned} n^7 &= n^3 \times n^3 \times n \\ &\equiv n \times n \times n \\ &\equiv n^3 \equiv n\ [3]. \end{aligned}$$

Conclusion. $3 \mid n^7 - n$.

3.

Montre que $2 \mid n^7 - n$.

INDICE

Distingue deux cas, selon la parité de n, et calcule n^7 modulo 2 dans chaque cas.

CORRIGÉ

On raisonne par disjonction de cas sur le reste de n dans la division euclidienne par 2.

- Si $n \equiv 0\ [2]$, alors $n^7 \equiv 0\ [2]$, donc $n^7 - n \equiv 0 - 0 = 0\ [2]$.
- Si $n \equiv 1\ [2]$, alors $n^7 \equiv 1\ [2]$, donc $n^7 - n \equiv 1 - 1 = 0\ [2]$.

Conclusion. Dans les deux cas, $2 \mid n^7 - n$.

4.

Déduis-en que $42 \mid n^7 - n$. Nomme précisément la propriété utilisée et vérifie ses hypothèses.

INDICE

Utilise la conséquence du théorème de Gauss sur deux diviseurs premiers entre eux, en deux temps : d'abord avec 2 et 3, puis avec 6 et 7.

CORRIGÉ

On note $N = n^7 - n$.

Propriété utilisée. Conséquence du théorème de Gauss : soient a, b et N des entiers ; si $a \mid N$, $b \mid N$ et $a \wedge b = 1$, alors $ab \mid N$.

Étape 1. On a $2 \mid N$ et $3 \mid N$ (questions 3 et 2). De plus, $2 \wedge 3 = 1$, car $3 - 2 = 1$ (théorème de Bézout). Donc $6 \mid N$.

Étape 2. On a $6 \mid N$ et $7 \mid N$ (question 1). De plus, $6 \wedge 7 = 1$, car 7 est premier et ne divise pas 6. Donc $42 \mid N$.

Conclusion. Pour tout entier relatif n, $42 \mid n^7 - n$.

5.

Application : donne le reste de 13^7 dans la division euclidienne par 42.

INDICE

D'après la question 4, $13^7 - 13$ est un multiple de 42. Pense ensuite à l'encadrement du reste.

CORRIGÉ

D'après la question 4 avec $n = 13$, $42 \mid 13^7 - 13$. Donc $13^7 \equiv 13 \ [42]$.

Conclusion. Comme $0 \leq 13 < 42$, le reste de 13^7 dans la division euclidienne par 42 est 13.

Exercice 8

Critères de divisibilité en base huit

Soit $N = \overline{a_k a_{k-1} \dots a_1 a_0}^{(8)}$ un entier naturel écrit en base 8. Ses chiffres vérifient $0 \leq a_i \leq 7$, et $N = a_k 8^k + \dots + a_1 \times 8 + a_0$.

1.

Montre que, pour tout entier naturel i, on a $8^i \equiv 1\ [7]$ et $8^i \equiv (-1)^i\ [9]$.

INDICE

Écris d'abord 8 modulo 7 et modulo 9, puis élève à la puissance i.

CORRIGÉ

Réduction de 8. On a $8 = 7 + 1$, donc $8 \equiv 1\ [7]$. De même, $8 = 9 - 1$, donc $8 \equiv -1\ [9]$.

Passage à la puissance. Une congruence se conserve par passage à la puissance. Soit $i \in \mathbb{N}$:

$$8^i \equiv 1^i = 1\ [7],$$
$$8^i \equiv (-1)^i\ [9].$$

Conclusion. Pour tout entier naturel i, $8^i \equiv 1\ [7]$ et $8^i \equiv (-1)^i\ [9]$.

2.

Déduis-en que $N \equiv a_0 + a_1 + \dots + a_k\ [7]$. Énonce un critère de divisibilité par 7 d'un entier écrit en base 8.

INDICE

Remplace chaque 8^i par 1 dans l'écriture de N, en utilisant la compatibilité des congruences avec la somme et le produit.

CORRIGÉ

Terme à terme. Soit $i \in \{0, \dots, k\}$. D'après la question 1, $8^i \equiv 1\ [7]$, donc $a_i \times 8^i \equiv a_i\ [7]$.

Somme. Par compatibilité des congruences avec la somme :

$$\begin{aligned} N &= a_k 8^k + \dots \\ &\quad + a_1 \times 8 + a_0 \\ &\equiv a_k + \dots + a_1 + a_0\ [7]. \end{aligned}$$

Critère. Deux entiers congrus modulo 7 sont tous deux divisibles par 7, ou aucun ne l'est.

Conclusion. $N \equiv a_0 + a_1 + \dots + a_k\ [7]$. Un entier écrit en base 8 est divisible par 7 si et seulement si la somme de ses chiffres en base 8 est divisible par 7.

3.

Montre de même que $N \equiv a_0 - a_1 + a_2 - \cdots + (-1)^k a_k \ [9]$.

INDICE

Cette fois, chaque 8^i se remplace par $(-1)^i$: regarde le signe obtenu pour i pair et pour i impair.

CORRIGÉ

Soit $i \in \{0, \ldots, k\}$. D'après la question 1, $a_i \times 8^i \equiv (-1)^i a_i \ [9]$: le signe est $+$ pour i pair et $-$ pour i impair.

En additionnant ces congruences :

$$\begin{aligned} N \equiv a_0 - a_1 + a_2 - \ldots \\ + (-1)^k a_k \ [9]. \end{aligned}$$

Conclusion. $N \equiv a_0 - a_1 + a_2 - \cdots + (-1)^k a_k \ [9]$.

4.

Soit $M = \overline{53627}^{(8)}$. Sans convertir M en base dix, donne les restes de M dans les divisions euclidiennes par 7 et par 9. Contrôle ensuite en convertissant.

INDICE

Lis les chiffres de droite à gauche : $a_0 = 7$, $a_1 = 2$, et ainsi de suite. Réduis ensuite les sommes obtenues pour arriver à des restes encadrés.

CORRIGÉ

Les chiffres de M, lus de droite à gauche, sont $a_0 = 7$, $a_1 = 2$, $a_2 = 6$, $a_3 = 3$ et $a_4 = 5$.

Modulo 7. D'après la question 2, on somme les chiffres : $7 + 2 + 6 + 3 + 5 = 23$, et $23 = 7 \times 3 + 2$. Donc $M \equiv 2 \ [7]$. Comme $0 \leq 2 < 7$, le reste est 2.

Modulo 9. D'après la question 3, on forme la somme alternée : $7 - 2 + 6 - 3 + 5 = 13$, et $13 = 9 \times 1 + 4$. Donc $M \equiv 4 \ [9]$. Comme $0 \leq 4 < 9$, le reste est 4.

Contrôle. En base dix :

$$\begin{aligned} M &= 5 \times 8^4 + 3 \times 8^3 \\ &\quad + 6 \times 8^2 + 2 \times 8 + 7 \\ &= 20480 + 1536 + 384 \\ &\quad + 16 + 7 \\ &= 22423. \end{aligned}$$

Or $22423 = 7 \times 3203 + 2$ et $22423 = 9 \times 2491 + 4$.

Conclusion. Les restes de M dans les divisions euclidiennes par 7 et par 9 sont respectivement 2 et 4.

5.

Détermine le chiffre c de la base 8 tel que l'entier $\overline{4c15}^{(8)}$ soit divisible par 7.

INDICE

Applique le critère de la question 2. N'oublie pas que c est un chiffre de la base 8 : $0 \leq c \leq 7$.

CORRIGÉ

D'après la question 2 :

$$\begin{aligned}\overline{4c15}^{(8)} &\equiv 4 + c + 1 + 5 \\ &\equiv 10 + c \ [7].\end{aligned}$$

Comme $10 \equiv 3 \ [7]$, l'entier est divisible par 7 si et seulement si $c + 3 \equiv 0 \ [7]$, soit $c \equiv 4 \ [7]$.

Or c est un chiffre de la base 8 : $0 \leq c \leq 7$. Le seul entier de cet intervalle congru à 4 modulo 7 est 4.

Contrôle. $\overline{4415}^{(8)} = 4 \times 512 + 4 \times 64 + 1 \times 8 + 5 = 2317$, et $2317 = 7 \times 331$.

Conclusion. Le chiffre cherché est $c = 4$.