BURHAN

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

2ème Année Baccalauréat · Sciences Mathématiques · Mathématiques

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

Chapitre	Palier	Exercices
Arithmétique dans $\mathbb{Z}$	Application	11

Exercice 1

Un écart de carrés et un reste négatif

1.

Montre que, pour tout entier relatif n, l'entier $(n+3)^2-(n-4)^2$ est un multiple de 7.

INDICE

Reconnais une différence de deux carrés : $A^2-B^2=(A-B)(A+B)$. Calcule d'abord $A-B$ avec $A=n+3$ et $B=n-4$.

CORRIGÉ

Soit $n\in\mathbb{Z}$. On cherche à écrire $(n+3)^2-(n-4)^2$ comme 7 fois un entier.

Factorisation. Posons $A=n+3$ et $B=n-4$. Alors $A-B=7$ et $A+B=2n-1$. D'après l'identité $A^2-B^2=(A-B)(A+B)$:

$$\begin{aligned}&(n+3)^2-(n-4)^2\\&=(A-B)(A+B)\\&=7(2n-1).\end{aligned}$$

Conclusion. Comme $2n-1$ est un entier relatif, la définition de la divisibilité donne $7\mid(n+3)^2-(n-4)^2$. Ceci vaut pour tout $n\in\mathbb{Z}$.

2.

Écris la division euclidienne de -250 par 9. Précise le quotient et le reste.

INDICE

Divise d'abord 250 par 9, puis change les signes. Le point délicat : le reste doit vérifier $0\le r<9$. S'il sort négatif, il faut encore ajuster le quotient.

CORRIGÉ

Division de 250. On a $250=9\times27+7$. En changeant les signes :

$$-250=9\times(-27)-7.$$

Ce n'est pas une division euclidienne : le reste doit être positif ou nul, et $-7<0$.

Ajustement du quotient. On écrit $-7=-9+2$:

$$\begin{aligned}-250&=9\times(-27)-9+2\\&=9\times(-28)+2.\end{aligned}$$

Conclusion. Comme $0\le2<9$, c'est bien la division euclidienne de -250 par 9. Le quotient est $q=-28$ et le reste est $r=2$.

3.

Détermine les entiers naturels n tels que $n+2$ divise $3n+17$.

INDICE

Écris $3n+17$ sous la forme $3(n+2)+c$, avec un entier c à trouver. Un diviseur commun à deux entiers divise toute combinaison de ces deux entiers.

CORRIGÉ

Soit $n \in \mathbb{N}$. On remarque que $3n+17 = 3(n+2)+11$.

Condition nécessaire. Supposons que $n+2$ divise $3n+17$. Comme $n+2$ divise aussi $n+2$, il divise toute combinaison de ces deux entiers, en particulier :

$$(3n+17) - 3(n+2) = 11.$$

Les diviseurs positifs de 11 sont 1 et 11. Or $n+2 \geq 2$, donc $n+2 = 11$, soit $n = 9$.

Réciproque. Pour $n = 9$: $n+2 = 11$ et $3n+17 = 44 = 11 \times 4$. Donc $11 \mid 44$.

Conclusion. Un seul entier naturel convient : $n = 9$.

Exercice 2

Les puissances de 5 modulo 13

1.

Recopie et complète le tableau des restes de 5^k dans la division euclidienne par 13.

k	1	2	3	4
reste de 5^k	?	?	?	?

INDICE

Ne calcule jamais 5^k en entier : multiplie le reste précédent par 5, puis réduis le produit modulo 13.

CORRIGÉ

On ne calcule jamais 5^k en entier : on multiplie le reste précédent par 5, puis on réduit modulo 13. On utilise $25 = 13 \times 1 + 12$, $60 = 13 \times 4 + 8$ et $40 = 13 \times 3 + 1$:

$$\begin{aligned} 5^2 &= 25 \equiv 12 \ [13] \\ 5^3 &\equiv 12 \times 5 \\ &= 60 \equiv 8 \ [13] \\ 5^4 &\equiv 8 \times 5 \\ &= 40 \equiv 1 \ [13] \end{aligned}$$

Chaque nombre obtenu est compris entre 0 et 12 : c'est donc le reste cherché.

Conclusion. Le tableau complété est le suivant.

k	1	2	3	4
reste de 5^k	5	12	8	1

2.

Déduis-en le reste de la division euclidienne de 5^{2026} par 13.

INDICE

Le cycle a pour longueur 4, car $5^4 \equiv 1 \ [13]$. Écris la division euclidienne de l'exposant 2026 par 4.

CORRIGÉ

Réduction de l'exposant. La division euclidienne de 2026 par 4 s'écrit $2026 = 4 \times 506 + 2$, avec $0 \leq 2 < 4$.

Calcul modulo 13. D'après la question 1, $5^4 \equiv 1 \ [13]$ et $5^2 \equiv 12 \ [13]$. Les congruences sont compatibles avec le produit et les puissances :

$$\begin{aligned} 5^{2026} &= \left(5^4\right)^{506} \times 5^2 \\ &\equiv 1^{506} \times 12 \ [13] \\ &\equiv 12 \ [13]. \end{aligned}$$

Conclusion. Comme $0 \leq 12 < 13$, le reste de la division euclidienne de 5^{2026} par 13 est 12.

3.

Montre que, pour tout entier naturel n, l'entier $5^{4n+3}+5$ est divisible par 13.

INDICE

Écris $5^{4n+3}=\left(5^4\right)^n\times 5^3$ et utilise le tableau de la question 1.

CORRIGÉ

Soit $n\in\mathbb{N}$. D'après la question 1, $5^4\equiv 1\ [13]$ et $5^3\equiv 8\ [13]$. Par compatibilité des congruences avec le produit et les puissances :

$$\begin{aligned}&5^{4n+3}+5\\&=\left(5^4\right)^n\times 5^3+5\\&\equiv 1^n\times 8+5\\&=13\equiv 0\ [13].\end{aligned}$$

Conclusion. Pour tout entier naturel n, on a $13\mid 5^{4n+3}+5$.

4.

Quel est le reste de 18^{2026} dans la division euclidienne par 13 ?

INDICE

Cherche un entier plus simple qui soit congru à 18 modulo 13.

CORRIGÉ

Réduction de la base. On a $18=13\times 1+5$, donc $18\equiv 5\ [13]$.

Passage à la puissance. Une congruence se conserve par passage à la puissance :

$$18^{2026}\equiv 5^{2026}\ [13].$$

D'après la question 2, $5^{2026}\equiv 12\ [13]$. Donc $18^{2026}\equiv 12\ [13]$.

Conclusion. Comme $0\leq 12<13$, le reste de 18^{2026} dans la division euclidienne par 13 est 12.

Exercice 3

383 et 1147 : premier ou composé ?

1.

Montre que 383 est un nombre premier.

INDICE

Liste d'abord les nombres premiers p tels que $p^2 \leq 383$: compare 383 aux carrés 17^2, 19^2 et 23^2. Teste ensuite chacun de ces premiers.

CORRIGÉ

Les premiers à tester. On a $19^2 = 361$ et $23^2 = 529$, donc $19^2 \leq 383 < 23^2$. Les nombres premiers p tels que $p^2 \leq 383$ sont donc 2, 3, 5, 7, 11, 13, 17 et 19.

Divisions. On divise 383 par chacun d'eux :

p	division euclidienne	reste
2	$383 = 2 \times 191 + 1$	1
3	$383 = 3 \times 127 + 2$	2
5	$383 = 5 \times 76 + 3$	3
7	$383 = 7 \times 54 + 5$	5
11	$383 = 11 \times 34 + 9$	9
13	$383 = 13 \times 29 + 6$	6
17	$383 = 17 \times 22 + 9$	9
19	$383 = 19 \times 20 + 3$	3

Chaque reste vérifie $0 \leq r < p$, et aucun n'est nul.

Conclusion. Aucun nombre premier p tel que $p^2 \leq 383$ ne divise 383. D'après la propriété du plus petit diviseur premier, 383 est premier.

2.

Détermine le plus petit diviseur premier de 1147.

INDICE

Teste les nombres premiers dans l'ordre croissant : le premier qui divise 1147 est son plus petit diviseur premier. Tu n'iras pas au-delà des premiers p tels que $p^2 \leq 1147$.

CORRIGÉ

Méthode. On teste les nombres premiers dans l'ordre croissant. Le premier qui divise 1147 est son plus petit diviseur premier.

p	division euclidienne	reste
2	$1147 = 2 \times 573 + 1$	1
3	$1147 = 3 \times 382 + 1$	1
5	$1147 = 5 \times 229 + 2$	2
7	$1147 = 7 \times 163 + 6$	6
11	$1147 = 11 \times 104 + 3$	3
13	$1147 = 13 \times 88 + 3$	3
17	$1147 = 17 \times 67 + 8$	8
19	$1147 = 19 \times 60 + 7$	7
23	$1147 = 23 \times 49 + 20$	20
29	$1147 = 29 \times 39 + 16$	16
31	$1147 = 31 \times 37 + 0$	0

Chaque reste vérifie $0 \leq r < p$. Aucun nombre premier strictement inférieur à 31 ne divise 1147, et 31 le divise.

31 **est premier.** On a $5^2 = 25 \leq 31 < 49 = 7^2$: les premiers p tels que $p^2 \leq 31$ sont 2, 3 et 5. Or $31 = 2 \times 15 + 1$, $31 = 3 \times 10 + 1$ et $31 = 5 \times 6 + 1$. Aucun ne divise 31, donc 31 est premier.

Conclusion. Le plus petit diviseur premier de 1147 est 31.

3.

Déduis-en que 1147 est composé, puis montre que 1147 est le produit de deux nombres premiers.

INDICE

Écris le quotient de 1147 par 31. Pour savoir si ce quotient est premier, il suffit de tester les premiers p dont le carré ne le dépasse pas.

CORRIGÉ

1147 **est composé.** D'après la question 2, $1147 = 31 \times 37$, avec $1 < 31 < 1147$. L'entier 1147 admet un diviseur autre que 1 et lui-même : il est composé.

37 **est premier.** On a $5^2 = 25 \leq 37 < 49 = 7^2$: les premiers p tels que $p^2 \leq 37$ sont 2, 3 et 5. Or $37 = 2 \times 18 + 1$, $37 = 3 \times 12 + 1$ et $37 = 5 \times 7 + 2$. Chaque reste vérifie $0 \leq r < p$ et n'est pas nul : aucun de ces premiers ne divise 37, donc 37 est premier.

Conclusion. L'entier 1147 est composé. Comme 31 est premier (question 2) et 37 aussi, $1147 = 31 \times 37$ est le produit de deux nombres premiers.

Exercice 4

L'algorithme d'Euclide pour 1716 et 1001

1.

Calcule $1716 \wedge 1001$ par l'algorithme d'Euclide. Présente les divisions successives dans un tableau.

INDICE

Divise 1716 par 1001, puis 1001 par le reste obtenu, et continue tant que le reste n'est pas nul. Sur chaque ligne, le reste est strictement inférieur au diviseur.

CORRIGÉ

On enchaîne les divisions euclidiennes : chacune divise le diviseur précédent par le reste obtenu.

étape	division euclidienne	reste
1	$1716 = 1001 \times 1 + 715$	715
2	$1001 = 715 \times 1 + 286$	286
3	$715 = 286 \times 2 + 143$	143
4	$286 = 143 \times 2 + 0$	0

Sur chaque ligne, le reste est compris entre 0 inclus et le diviseur exclu.

Conclusion. Le PGCD est le dernier reste non nul :

$$1716 \wedge 1001 = 143.$$

2.

Déduis-en $1716 \vee 1001$.

INDICE

Pour deux entiers naturels non nuls, le produit de leur PGCD par leur PPCM est égal au produit des deux entiers. Simplifie avant de multiplier.

CORRIGÉ

Propriété utilisée. Pour deux entiers naturels non nuls a et b :

$$(a \wedge b)(a \vee b) = ab.$$

Calcul. D'après la question 1, $1716 \wedge 1001 = 143$. De plus $1716 = 143 \times 12$, donc :

$$\begin{aligned} 1716 \vee 1001 &= \frac{1716 \times 1001}{143} \\ &= 12 \times 1001 \\ &= 12012. \end{aligned}$$

Conclusion. Le PPCM vaut $1716 \vee 1001 = 12012$.

3.

Écris la fraction $\dfrac{1001}{1716}$ sous forme irréductible.

INDICE

Divise le numérateur et le dénominateur par leur PGCD. Justifie ensuite que les deux quotients obtenus sont premiers entre eux.

CORRIGÉ

Simplification. D'après la question 1, le PGCD de 1001 et 1716 est 143. Or $1001 = 143 \times 7$ et $1716 = 143 \times 12$, donc :

$$\frac{1001}{1716} = \frac{7}{12}.$$

Irréductibilité. Le nombre 7 est premier et ne divise pas 12, car $12 = 7 \times 1 + 5$ avec $0 < 5 < 7$. Donc $7 \wedge 12 = 1$.

Conclusion. La forme irréductible de $\dfrac{1001}{1716}$ est $\dfrac{7}{12}$.

Exercice 5

Un couple de Bézout pour 157 et 68

1.

Applique l'algorithme d'Euclide à 157 et 68. Que vaut $157 \wedge 68$?

INDICE

Enchaîne les divisions euclidiennes jusqu'à obtenir un reste nul. Écris chaque division avec son reste encadré.

CORRIGÉ

On enchaîne les divisions euclidiennes :

division euclidienne	reste
$157 = 68 \times 2 + 21$	21
$68 = 21 \times 3 + 5$	5
$21 = 5 \times 4 + 1$	1
$5 = 1 \times 5 + 0$	0

Chaque reste est positif ou nul et strictement inférieur à son diviseur.

Conclusion. Le dernier reste non nul est 1, donc $157 \wedge 68 = 1$.

2.

Remonte les divisions de la question 1 pour obtenir un couple (u, v) d'entiers relatifs tel que $157u + 68v = 1$. Vérifie ton résultat.

INDICE

Pars de la dernière division utile : $1 = 21 - 4 \times 5$. Remplace ensuite 5 par son expression tirée de la ligne au-dessus. Garde 21, 68 et 157 comme des « briques », sans effectuer les produits.

CORRIGÉ

Restes isolés. Les trois premières divisions de la question 1 donnent :

$$\begin{aligned} 21 &= 157 - 2 \times 68 \\ 5 &= 68 - 3 \times 21 \\ 1 &= 21 - 4 \times 5 \end{aligned}$$

Remontée. On part de la dernière égalité et on remplace de bas en haut, sans effectuer les produits :

$$\begin{aligned} 1 &= 21 - 4 \times 5 \\ &= 21 - 4 \times (68 - 3 \times 21) \\ &= 13 \times 21 - 4 \times 68 \\ &= 13 \times (157 - 2 \times 68) \\ &\quad - 4 \times 68 \\ &= 13 \times 157 - 30 \times 68. \end{aligned}$$

Vérification. On a $157 \times 13 = 2041$ et $68 \times 30 = 2040$, donc $157 \times 13 + 68 \times (-30) = 1$.

Conclusion. Le couple $(u, v) = (13, -30)$ vérifie $157u + 68v = 1$.

3.

Soit n un entier naturel. Montre que $3n + 5$ et $2n + 3$ sont premiers entre eux.

INDICE

Cherche des entiers u et v, indépendants de n, tels que les termes en n s'éliminent dans $u(3n + 5) + v(2n + 3)$.

CORRIGÉ

Soit $n \in \mathbb{N}$. On cherche une combinaison à coefficients entiers de $3n + 5$ et $2n + 3$ qui élimine n :

$$\begin{aligned} &2(3n + 5) - 3(2n + 3) \\ &= 6n + 10 - 6n - 9 \\ &= 1. \end{aligned}$$

Théorème de Bézout. Les entiers $u = 2$ et $v = -3$ vérifient donc :

$$(3n + 5)u + (2n + 3)v = 1.$$

D'après le théorème de Bézout, $(3n + 5) \wedge (2n + 3) = 1$.

Conclusion. Pour tout entier naturel n, les entiers $3n + 5$ et $2n + 3$ sont premiers entre eux.

Exercice 6

Gauss, avec et sans son hypothèse

1.

Soit n un entier relatif tel que $9 \mid 14n$. Montre que $9 \mid n$.

INDICE

Pense au théorème de Gauss. Avant de l'appliquer, prouve que 9 et 14 sont premiers entre eux, par exemple avec une combinaison égale à 1.

CORRIGÉ

Soit $n \in \mathbb{Z}$ tel que $9 \mid 14n$.

9 et 14 sont premiers entre eux. On a $2 \times 14 - 3 \times 9 = 28 - 27 = 1$. D'après le théorème de Bézout, $9 \wedge 14 = 1$.

Théorème de Gauss. L'entier 9 divise le produit $14n$ et il est premier avec 14. D'après le théorème de Gauss, 9 divise n.

Conclusion. Pour tout entier relatif n, si $9 \mid 14n$, alors $9 \mid n$.

2.

Un élève écrit : « 6 divise 4×9, donc 6 divise 9. » Montre que sa conclusion est fausse et indique l'hypothèse du théorème de Gauss qui n'est pas vérifiée.

INDICE

Calcule 4×9 et regarde sa divisibilité par 6. Calcule ensuite le PGCD de 6 et de 4.

CORRIGÉ

La conclusion est fausse. On a $4 \times 9 = 36$ et $36 = 6 \times 6$, donc $6 \mid 4 \times 9$. Mais $9 = 6 \times 1 + 3$, avec $0 < 3 < 6$: le reste n'est pas nul, donc $6 \nmid 9$.

L'hypothèse manquante. Pour déduire $6 \mid 9$ de $6 \mid 4 \times 9$, le théorème de Gauss exige que 6 et 4 soient premiers entre eux. Or $6 \wedge 4 = 2$.

Conclusion. L'élève se trompe : 6 divise 4×9 sans diviser 9. L'hypothèse de primalité relative $6 \wedge 4 = 1$ du théorème de Gauss n'est pas vérifiée.

3.

Détermine tous les couples (x, y) d'entiers relatifs tels que $9x = 14y$.

INDICE

L'égalité montre que 9 divise $14y$. La question 1 te dit ce que tu peux en conclure pour y. N'oublie pas de vérifier la réciproque.

CORRIGÉ

Analyse. Soit $(x, y) \in \mathbb{Z}^2$ tel que $9x = 14y$. Alors $9 \mid 14y$. Comme $9 \wedge 14 = 1$ (question 1), le théorème de Gauss donne $9 \mid y$. Il existe donc $k \in \mathbb{Z}$ tel que $y = 9k$.

En remplaçant, $9x = 14 \times 9k$. On simplifie par $9 \neq 0$: $x = 14k$.

Synthèse. Soit $k \in \mathbb{Z}$. Le couple $(14k, 9k)$ vérifie $9 \times 14k = 14 \times 9k$: c'est une solution.

Conclusion. Les couples d'entiers relatifs (x, y) tels que $9x = 14y$ sont les couples $(14k, 9k)$, avec $k \in \mathbb{Z}$.

Exercice 7

1260 et 1350 décomposés

1.

Décompose 1260 et 1350 en produits de facteurs premiers.

INDICE

Divise successivement par les plus petits nombres premiers possibles : 2, puis 3, puis 5, puis 7.

CORRIGÉ

On divise par les plus petits nombres premiers possibles, tant que c'est possible.

Décomposition de 1260.

$$\begin{aligned} 1260 &= 2 \times 630 \\ &= 2^2 \times 315 \\ &= 2^2 \times 3 \times 105 \\ &= 2^2 \times 3^2 \times 35 \\ &= 2^2 \times 3^2 \times 5 \times 7. \end{aligned}$$

Décomposition de 1350.

$$\begin{aligned} 1350 &= 2 \times 675 \\ &= 2 \times 3 \times 225 \\ &= 2 \times 3^2 \times 75 \\ &= 2 \times 3^3 \times 25 \\ &= 2 \times 3^3 \times 5^2. \end{aligned}$$

Conclusion. Les facteurs 2, 3, 5 et 7 sont premiers : les décompositions cherchées sont $1260 = 2^2 \times 3^2 \times 5 \times 7$ et $1350 = 2 \times 3^3 \times 5^2$.

2.

Combien l'entier 1260 a-t-il de diviseurs positifs ?

INDICE

Un diviseur positif de 1260 s'écrit $2^{\beta_1} \times 3^{\beta_2} \times 5^{\beta_3} \times 7^{\beta_4}$. Compte les valeurs possibles de chaque exposant, sans oublier la valeur 0.

CORRIGÉ

Forme des diviseurs. D'après la question 1, $1260 = 2^2 \times 3^2 \times 5^1 \times 7^1$. Par unicité de la décomposition, les diviseurs positifs d de 1260 sont les entiers :

$$\begin{aligned} d = 2^{\beta_1} \times 3^{\beta_2} \\ \times 5^{\beta_3} \times 7^{\beta_4}, \end{aligned}$$

avec $0 \leq \beta_1 \leq 2$, $0 \leq \beta_2 \leq 2$, $0 \leq \beta_3 \leq 1$ et $0 \leq \beta_4 \leq 1$. Deux choix distincts d'exposants donnent deux diviseurs distincts.

Dénombrement. On multiplie les nombres de choix de chaque exposant :

$$\begin{aligned} &(2+1)(2+1)(1+1)(1+1) \\ &= 36. \end{aligned}$$

Conclusion. L'entier 1260 a 36 diviseurs positifs.

3.

Calcule $1260 \wedge 1350$ et $1260 \vee 1350$ à l'aide des décompositions, puis contrôle tes résultats.

INDICE

Écris les deux décompositions avec les mêmes nombres premiers $2, 3, 5, 7$, en acceptant des exposants nuls. Le PGCD prend le plus petit exposant de chaque premier, le PPCM le plus grand.

CORRIGÉ

Décompositions sur les mêmes premiers. On accepte l'exposant 0 :

$$\begin{aligned} 1260 &= 2^2 \times 3^2 \times 5^1 \times 7^1 \\ 1350 &= 2^1 \times 3^3 \times 5^2 \times 7^0 \end{aligned}$$

PGCD et PPCM. Le PGCD prend le plus petit exposant de chaque premier, le PPCM le plus grand :

$$\begin{aligned} &1260 \wedge 1350 \\ &= 2^1 \times 3^2 \times 5^1 \times 7^0 \\ &= 90, \\ &1260 \vee 1350 \\ &= 2^2 \times 3^3 \times 5^2 \times 7^1 \\ &= 18900. \end{aligned}$$

Contrôle. On a $90 \times 18900 = 1\,701\,000$ et $1260 \times 1350 = 1\,701\,000$. On retrouve $(a \wedge b)(a \vee b) = ab$, avec $a = 1260$ et $b = 1350$.

Conclusion. Le PGCD de 1260 et 1350 vaut 90, leur PPCM vaut 18900.

4.

Quel est le plus petit entier naturel non nul k tel que $1260k$ soit le carré d'un entier ?

INDICE

Par l'unicité de la décomposition, un entier naturel non nul est un carré exactement quand tous les exposants de sa décomposition sont pairs. Repère les exposants impairs de 1260.

CORRIGÉ

Condition nécessaire. Soit $k \in \mathbb{N}^*$ tel que $1260k = m^2$, avec $m \in \mathbb{N}$. Dans la décomposition de m^2, tous les exposants sont pairs.

L'exposant de 5 dans $1260k$ vaut 1 plus l'exposant de 5 dans k. Il n'est pair que si $5 \mid k$. De même, $7 \mid k$.

Comme 5 et 7 sont deux premiers distincts, $5 \wedge 7 = 1$. D'après la conséquence du théorème de Gauss (deux diviseurs premiers entre eux de k ont leur produit qui divise k), $35 \mid k$. Comme $k > 0$, on obtient $k \geq 35$.

Réciproque. Pour $k = 35$:

$$\begin{aligned} & 1260 \times 35 \\ & = 2^2 \times 3^2 \times 5^2 \times 7^2 \\ & = 44100 \\ & = 210^2. \end{aligned}$$

Conclusion. Le plus petit entier naturel non nul qui convient est $k = 35$.

Exercice 8

La table de multiplication modulo 10

1.

Dresse la table de multiplication de $\mathbb{Z}/10\mathbb{Z}$.

INDICE

Dans la case de la ligne $\overline{a}$ et de la colonne $\overline{b}$, calcule ab, puis prends son reste dans la division par 10. La table est symétrique : la moitié des cases suffit.

CORRIGÉ

Soient a et b deux entiers tels que $0 \leq a \leq 9$ et $0 \leq b \leq 9$. La case de la ligne $\overline{a}$ et de la colonne $\overline{b}$ contient :

$$\overline{a} \times \overline{b} = \overline{ab} = \overline{r},$$

où r est le reste de la division euclidienne de ab par 10. Par exemple, $7 \times 8 = 56 = 10 \times 5 + 6$, donc $\overline{7} \times \overline{8} = \overline{6}$.

Conclusion. La table de multiplication de $\mathbb{Z}/10\mathbb{Z}$ est la suivante.

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{6}$	$\overline{8}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{6}$	$\overline{8}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{9}$	$\overline{2}$	$\overline{5}$	$\overline{8}$	$\overline{1}$	$\overline{4}$	$\overline{7}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{8}$	$\overline{2}$	$\overline{6}$	$\overline{0}$	$\overline{4}$	$\overline{8}$	$\overline{2}$	$\overline{6}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{0}$	$\overline{5}$
$\overline{6}$	$\overline{0}$	$\overline{6}$	$\overline{2}$	$\overline{8}$	$\overline{4}$	$\overline{0}$	$\overline{6}$	$\overline{2}$	$\overline{8}$	$\overline{4}$
$\overline{7}$	$\overline{0}$	$\overline{7}$	$\overline{4}$	$\overline{1}$	$\overline{8}$	$\overline{5}$	$\overline{2}$	$\overline{9}$	$\overline{6}$	$\overline{3}$
$\overline{8}$	$\overline{0}$	$\overline{8}$	$\overline{6}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{8}$	$\overline{6}$	$\overline{4}$	$\overline{2}$
$\overline{9}$	$\overline{0}$	$\overline{9}$	$\overline{8}$	$\overline{7}$	$\overline{6}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

2.

Lis dans la table les classes inversibles de $\mathbb{Z}/10\mathbb{Z}$ et donne l'inverse de chacune. Contrôle avec la caractérisation par le PGCD.

INDICE

Une classe $\overline{a}$ est inversible lorsque sa ligne contient la classe $\overline{1}$. Pour le contrôle, calcule $a \wedge 10$ pour chaque a de 0 à 9.

CORRIGÉ

Lecture de la table. La classe $\overline{1}$ apparaît dans les lignes de $\overline{1}$, $\overline{3}$, $\overline{7}$ et $\overline{9}$:

$$\begin{aligned}\overline{1} \times \overline{1} &= \overline{1}\\ \overline{3} \times \overline{7} &= \overline{21} = \overline{1}\\ \overline{9} \times \overline{9} &= \overline{81} = \overline{1}\end{aligned}$$

Ces quatre classes sont inversibles. L'inverse de $\overline{3}$ est $\overline{7}$, celui de $\overline{7}$ est $\overline{3}$. Les classes $\overline{1}$ et $\overline{9}$ sont leur propre inverse.

Les lignes de $\overline{0}$, $\overline{2}$, $\overline{4}$, $\overline{5}$, $\overline{6}$ et $\overline{8}$ ne contiennent pas $\overline{1}$: ces classes ne sont pas inversibles.

Contrôle par le PGCD. On a $a \wedge 10 = 1$ pour $a = 1, 3, 7, 9$. Pour les autres valeurs : $0 \wedge 10 = 10$, $2 \wedge 10 = 2$, $4 \wedge 10 = 2$, $5 \wedge 10 = 5$, $6 \wedge 10 = 2$ et $8 \wedge 10 = 2$. On retrouve que $\overline{a}$ est inversible si et seulement si $a \wedge 10 = 1$.

Conclusion. Les classes inversibles de $\mathbb{Z}/10\mathbb{Z}$ sont $\overline{1}$, $\overline{3}$, $\overline{7}$ et $\overline{9}$, d'inverses respectifs $\overline{1}$, $\overline{7}$, $\overline{3}$ et $\overline{9}$.

3.

Résous dans $\mathbb{Z}/10\mathbb{Z}$ l'équation $\overline{3} \times x = \overline{7}$.

INDICE

Multiplie les deux membres par l'inverse de $\overline{3}$ trouvé à la question 2. Vérifie ensuite la classe obtenue.

CORRIGÉ

Analyse. Soit $x \in \mathbb{Z}/10\mathbb{Z}$ tel que $\overline{3} \times x = \overline{7}$. On multiplie les deux membres par $\overline{7}$, inverse de $\overline{3}$ (question 2) :

$$\begin{aligned}x &= \overline{7} \times \overline{3} \times x\\ &= \overline{7} \times \overline{7}\\ &= \overline{49} = \overline{9},\end{aligned}$$

car $49 = 10 \times 4 + 9$, avec $0 \leq 9 < 10$.

Vérification. On a $\overline{3} \times \overline{9} = \overline{27} = \overline{7}$, car $27 = 10 \times 2 + 7$.

Conclusion. Dans $\mathbb{Z}/10\mathbb{Z}$, l'équation $\overline{3} \times x = \overline{7}$ a une seule solution : $x = \overline{9}$.

4.

Explique, à l'aide de la table, pourquoi l'équation $\overline{2} \times x = \overline{5}$ n'a aucune solution dans $\mathbb{Z}/10\mathbb{Z}$. Prouve-le ensuite sans la table.

INDICE

Regarde quelles classes apparaissent sur la ligne de $\overline{2}$. Pour une preuve sans la table, cherche un diviseur commun à 2 et à 10.

CORRIGÉ

Avec la table. La ligne de $\overline{2}$ contient seulement $\overline{0}$, $\overline{2}$, $\overline{4}$, $\overline{6}$ et $\overline{8}$. La classe $\overline{5}$ n'y figure pas : aucune classe x ne vérifie $\overline{2} \times x = \overline{5}$.

Sans la table, par l'absurde. Supposons qu'il existe $c \in \mathbb{Z}$ tel que $\overline{2} \times \overline{c} = \overline{5}$. Alors $\overline{2c} = \overline{5}$, soit $2c \equiv 5\ [10]$. Donc $10 \mid 2c - 5$ et, comme $2 \mid 10$, $2 \mid 2c - 5$.

Comme $2 \mid 2c$, l'entier 2 divise la différence $2c - (2c - 5) = 5$. C'est faux.

Conclusion. L'équation $\overline{2} \times x = \overline{5}$ n'a aucune solution dans $\mathbb{Z}/10\mathbb{Z}$.

Exercice 9

Fermat pour une puissance de 7 modulo 11

1.

Justifie que $7^{10} \equiv 1\ [11]$, sans calculer 7^{10}.

INDICE

Pense au petit théorème de Fermat avec $p = 11$ et $a = 7$. Écris ses deux hypothèses et vérifie-les une à une.

CORRIGÉ

Le petit théorème de Fermat affirme : si p est premier et si p ne divise pas l'entier a, alors $a^{p-1} \equiv 1\ [p]$. On vérifie ses deux hypothèses pour $p = 11$ et $a = 7$.

- 11 **est premier.** Les premiers p tels que $p^2 \leq 11$ sont 2 et 3. Or $11 = 2 \times 5 + 1$ et $11 = 3 \times 3 + 2$: les restes ne sont pas nuls.
- $11 \nmid 7$**.** On a $7 = 11 \times 0 + 7$, avec $0 < 7 < 11$: le reste n'est pas nul.

Conclusion. D'après le petit théorème de Fermat, $7^{11-1} \equiv 1\ [11]$, c'est-à-dire $7^{10} \equiv 1\ [11]$.

2.

Déduis-en le reste de 7^{2025} dans la division euclidienne par 11.

INDICE

Réduis l'exposant modulo $p - 1 = 10$: écris $2025 = 10q + r$, avec $0 \leq r < 10$. Il te restera à calculer 7^r modulo 11 par petites étapes.

CORRIGÉ

Réduction de l'exposant. La division euclidienne de 2025 par 10 s'écrit $2025 = 10 \times 202 + 5$, avec $0 \leq 5 < 10$. Avec la question 1 :

$$\begin{aligned} 7^{2025} &= \left(7^{10}\right)^{202} \times 7^5 \\ &\equiv 1^{202} \times 7^5\ [11] \\ &\equiv 7^5\ [11]. \end{aligned}$$

Calcul de 7^5 modulo 11. On a $49 = 11 \times 4 + 5$, donc $7^2 \equiv 5\ [11]$. On élève au carré, puis on multiplie par 7 :

$$\begin{aligned} 7^4 &\equiv 5^2 = 25 \equiv 3\ [11] \\ 7^5 &\equiv 3 \times 7 = 21 \equiv 10\ [11] \end{aligned}$$

Conclusion. Comme $0 \leq 10 < 11$, le reste de la division euclidienne de 7^{2025} par 11 est 10.

3.

Montre que 11 divise $7^{2025}+1$.

INDICE

Utilise le résultat de la question 2 : à quoi est congru $7^{2025}+1$ modulo 11 ?

CORRIGÉ

D'après la question 2, $7^{2025} \equiv 10\ [11]$. Par compatibilité des congruences avec l'addition :

$$\begin{aligned} 7^{2025}+1 &\equiv 10+1=11 \\ &\equiv 0\ [11]. \end{aligned}$$

Conclusion. On a $7^{2025}+1 \equiv 0\ [11]$: l'entier 11 divise $7^{2025}+1$.

4.

Pourquoi la forme $a^{p-1} \equiv 1\ [p]$ du petit théorème de Fermat ne s'applique-t-elle pas à $a=33$ et $p=11$? Donne le reste de 33^{2025} dans la division par 11.

INDICE

Vérifie l'hypothèse « p ne divise pas a » pour $a=33$.

CORRIGÉ

Hypothèse non vérifiée. On a $33=11\times 3$, donc $11 \mid 33$. L'hypothèse « p ne divise pas a » du petit théorème de Fermat est en défaut : la forme $a^{p-1} \equiv 1\ [p]$ ne peut pas être utilisée.

Reste de 33^{2025}. Comme $33 \equiv 0\ [11]$, la compatibilité avec les puissances donne :

$$33^{2025} \equiv 0^{2025} = 0\ [11].$$

Conclusion. Le reste de 33^{2025} dans la division euclidienne par 11 est 0, et non 1.

Exercice 10

Compter en base six

1.

Écris en base 6 l'entier 1000 (donné en base dix).

INDICE

Divise 1000 par 6, puis le quotient par 6, et continue jusqu'à un quotient nul. Les restes, lus du dernier au premier, sont les chiffres.

CORRIGÉ

On divise successivement par 6, jusqu'à un quotient nul. Chaque reste vérifie $0 \leq r < 6$:

division euclidienne	reste
$1000 = 6 \times 166 + 4$	4
$166 = 6 \times 27 + 4$	4
$27 = 6 \times 4 + 3$	3
$4 = 6 \times 0 + 4$	4

Les restes, lus du dernier au premier, sont les chiffres en base 6 : $4, 3, 4, 4$.

Contrôle.

$$\begin{aligned} & 4 \times 6^3 + 3 \times 6^2 \\ & \quad + 4 \times 6 + 4 \\ & = 864 + 108 + 24 + 4 \\ & = 1000. \end{aligned}$$

Conclusion. En base 6, on a $1000 = \overline{4344}^{(6)}$.

2.

Écris en base dix l'entier $\overline{2153}^{(6)}$.

INDICE

Développe selon les puissances de 6 : le chiffre de droite est celui des unités, le suivant est multiplié par 6, puis par 6^2, et ainsi de suite.

CORRIGÉ

Les chiffres $2, 1, 5$ et 3 sont compris entre 0 et 5 : l'écriture a bien un sens en base 6. On développe selon les puissances de 6 :

$$\begin{aligned} \overline{2153}^{(6)} &= 2 \times 6^3 + 1 \times 6^2 \\ &\quad + 5 \times 6 + 3 \\ &= 432 + 36 + 30 + 3 \\ &= 501. \end{aligned}$$

Conclusion. En base dix, l'entier $\overline{2153}^{(6)}$ vaut 501.

3.

Pose l'addition $\overline{4344}^{(6)} + \overline{2153}^{(6)}$ directement en base 6, puis contrôle le résultat en base dix.

INDICE

Additionne colonne par colonne, de droite à gauche. Dès qu'une somme atteint 6, écris son reste par 6 et retiens le quotient.

CORRIGÉ

Addition posée. On additionne de droite à gauche. Quand une somme atteint 6, on écrit son reste par 6 et on retient le quotient :

colonne	calcul	chiffre écrit	retenue
unités	$4+3=7=6+1$	1	1
6	$4+5+1=10=6+4$	4	1
6^2	$3+1+1=5$	5	0
6^3	$4+2=6=6+0$	0	1

La dernière retenue donne le chiffre de 6^4 :

$$\begin{aligned}&\overline{4344}^{(6)} + \overline{2153}^{(6)}\\ &= \overline{10541}^{(6)}.\end{aligned}$$

Contrôle en base dix.

$$\begin{aligned}&\overline{10541}^{(6)}\\ &= 6^4 + 5\times 6^2\\ &\quad + 4\times 6 + 1\\ &= 1296 + 180 + 24 + 1\\ &= 1501.\end{aligned}$$

D'après les questions 1 et 2, on retrouve bien $1000 + 501 = 1501$.

Conclusion. La somme vaut $\overline{10541}^{(6)}$ en base 6, soit 1501 en base dix.

Exercice 11

Une équation en x et y, avec ou sans solution

1.

Montre que l'équation $12x + 18y = 7$ n'a aucune solution dans $\mathbb{Z}^2$.

INDICE

Calcule $12 \wedge 18$ et compare-le au second membre : l'existence de solutions dépend d'une divisibilité.

CORRIGÉ

PGCD. Par l'algorithme d'Euclide, $18 = 12 \times 1 + 6$ et $12 = 6 \times 2 + 0$, donc $12 \wedge 18 = 6$.

Divisibilité. On a $7 = 6 \times 1 + 1$, avec $0 < 1 < 6$: le reste n'est pas nul, donc $6 \nmid 7$. Or une équation $ax + by = c$ admet des solutions entières si et seulement si $a \wedge b$ divise c.

Vérification directe. Soit $(x, y) \in \mathbb{Z}^2$. L'entier $12x + 18y = 6(2x + 3y)$ est un multiple de 6, alors que 7 n'en est pas un.

Conclusion. L'équation $12x + 18y = 7$ n'a aucune solution dans $\mathbb{Z}^2$.

2.

On considère l'équation (E) : $12x + 18y = 30$. Justifie qu'elle admet des solutions, montre qu'elle équivaut à $2x + 3y = 5$ et trouve une solution évidente.

INDICE

Ici, le PGCD divise le second membre. Divise les deux membres de (E) par ce PGCD ; essaie ensuite de petites valeurs de x et de y.

CORRIGÉ

Existence. D'après la question 1, $12 \wedge 18 = 6$. Or $30 = 6 \times 5$, donc $6 \mid 30$: d'après le théorème d'existence, (E) admet des solutions dans $\mathbb{Z}^2$.

Équation simplifiée. Soit $(x, y) \in \mathbb{Z}^2$. On divise les deux membres par 6, qui est non nul :

$$\begin{aligned} & 12x + 18y = 30 \\ \iff\ & 2x + 3y = 5. \end{aligned}$$

Solution évidente. Le couple $(1, 1)$ convient, car $2 \times 1 + 3 \times 1 = 5$.

Conclusion. L'équation (E) a des solutions, elle équivaut à $2x + 3y = 5$, et $(1, 1)$ en est une.

3.

Détermine toutes les solutions de (E) dans $\mathbb{Z}^2$.

INDICE

Vérifie que 2 et 3 sont premiers entre eux. Le théorème qui décrit les solutions de $ax + by = c$ s'applique alors à partir de la solution $(1, 1)$.

CORRIGÉ

Hypothèses. On a $3 \times 1 - 2 \times 1 = 1$, donc $2 \wedge 3 = 1$ d'après le théorème de Bézout. Les entiers 2 et 3 sont non nuls et premiers entre eux. De plus, $(1, 1)$ est une solution de $2x + 3y = 5$ (question 2).

Solutions. D'après le théorème sur les solutions de $ax + by = c$, les solutions de $2x + 3y = 5$, donc de (E), sont les couples :

$$(1 + 3k,\ 1 - 2k), \quad k \in \mathbb{Z}.$$

Vérification. Soit $k \in \mathbb{Z}$:

$$\begin{aligned} &2(1 + 3k) + 3(1 - 2k) \\ &= 2 + 6k + 3 - 6k \\ &= 5. \end{aligned}$$

Conclusion. Les solutions de (E) dans $\mathbb{Z}^2$ sont les couples $(1 + 3k,\ 1 - 2k)$, où k parcourt $\mathbb{Z}$.