

Arithmétique dans $\mathbb{Z}$

Exercice 1 : Divisibilité et combinaisons linéaires

Dans cet exercice, a , b et n désignent des entiers relatifs.

1. Démontrez que si $a \mid b$ et $b \mid a$, alors $|a| = |b|$.
2. Déterminez tous les entiers n tels que $n + 3$ divise $2n + 13$.
3. Montrez que pour tout entier n , l'entier $n^2 + n$ est pair.

Exercice 2 : Division euclidienne et carrés modulo 4

1. Effectuez la division euclidienne de 2024 par 17, puis celle de -2024 par 17.
2. Effectuez la division euclidienne de -47 par 6.
3. Montrez que le reste de la division euclidienne d'un carré par 4 vaut 0 ou 1.
4. En déduire qu'aucun entier de la forme $4k + 3$ n'est somme de deux carrés d'entiers.

Exercice 3 : PGCD par l'algorithme d'Euclide

On souhaite paver un rectangle de 1071 sur 462 par des carrés tous identiques, dont le côté est un entier le plus grand possible. La figure ci-dessous représente ce rectangle.

462

rectangle à paver par des carrés
tous identiques, les plus grands possible

1071

1. Calculez $1071 \wedge 462$ par l'algorithme d'Euclide, en écrivant chaque division.
2. Expliquez pourquoi le côté cherché est ce PGCD, et donnez le nombre de carrés nécessaires.
3. Calculez de même $4620 \wedge 1386$.

Exercice 4 : Coefficients de Bézout

1. En remontant l'algorithme de l'exercice 3, trouvez des entiers u et v tels que $1071u + 462v = 21$.
2. Justifiez que 51 et 22 sont premiers entre eux.
3. Déterminez tous les couples $(u, v) \in \mathbb{Z}^2$ tels que $1071u + 462v = 21$.

Exercice 5 : Inverse modulaire par l'algorithme d'Euclide étendu

1. Appliquez l'algorithme d'Euclide à 97 et 35. Que vaut $97 \wedge 35$?

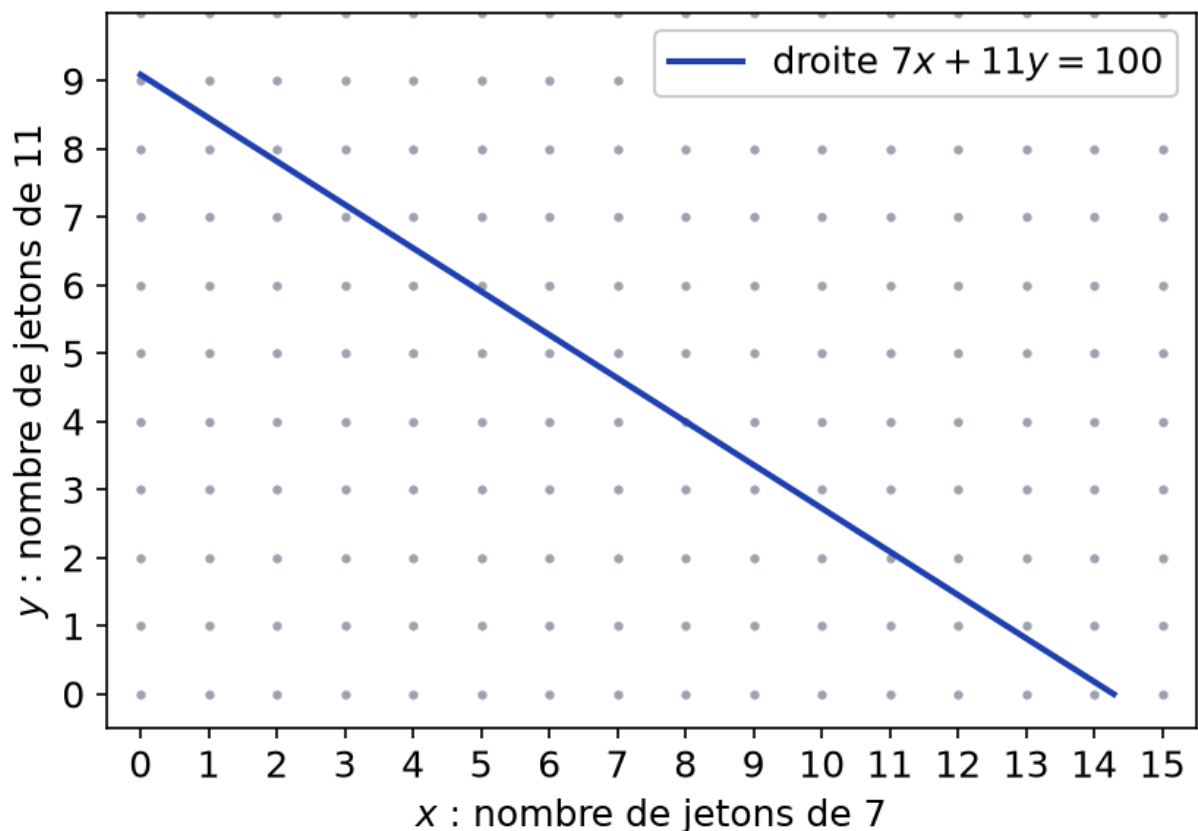
2. Remontez l'algorithme pour trouver des entiers u et v tels que $97u + 35v = 1$.
3. En déduire un inverse de 35 modulo 97 , compris entre 0 et 96 .
4. Résolvez dans $\mathbb{Z}$ la congruence $\begin{matrix} 35x \equiv 4 \\ , [97] \end{matrix}$.

Exercice 6 : Équation diophantienne $15x + 21y = c$

1. Montrez que l'équation $15x + 21y = 10$ n'a aucune solution entière.
2. Pour quels entiers c l'équation $15x + 21y = c$ a-t-elle des solutions entières ?
3. Résolvez dans $\mathbb{Z}^2$ l'équation $15x + 21y = 9$.
4. Déterminez la solution (x, y) de cette équation telle que $0 \leq x < 7$.

Exercice 7 : Atteindre 100 avec des jetons de 7 et de 11

Dans un jeu, on dispose de jetons de valeur 7 et de jetons de valeur 11 . On veut atteindre exactement la somme 100 . On note x le nombre de jetons de 7 et y le nombre de jetons de 11 . La figure ci-dessous représente la droite d'équation $7x + 11y = 100$ et le quadrillage des points à coordonnées entières positives.



1. Trouvez des entiers u et v tels que $7u + 11v = 1$, à l'aide de l'algorithme d'Euclide.
2. En déduire une solution particulière de $7x + 11y = 100$, puis toutes les solutions dans $\mathbb{Z}^2$.
3. Déterminez toutes les solutions avec $x \geq 0$ et $y \geq 0$. Combien de façons d'atteindre 100 existe-t-il ?

Exercice 8 : PGCD d'expressions dépendant de n

Dans cet exercice, n est un entier naturel.

1. Montrez que $(2n + 1) \wedge (3n + 2) = 1$.
2. Montrez que $(n + 1) \wedge (n^2 + n + 1) = 1$.
3. Montrez que $(n + 5) \wedge (2n + 3)$ vaut 1 ou 7.

4. Déterminez les entiers n pour lesquels ce PGCD vaut 7.

Exercice 9 : Lemme de Gauss et divisibilité

1. Montrez que si 7 divise $5n$, alors 7 divise n .
2. Résolvez dans $\mathbb{Z}^2$ l'équation $12x = 35y$.
3. Montrez que pour tout entier n , le produit $n(n+1)(2n+1)$ est divisible par 2 et par 3.
4. En déduire qu'il est divisible par 6, en citant précisément le résultat utilisé.

Exercice 10 : PGCD et PPCM imposés

1. Soient $a, b \in \mathbb{N}^*$ et $d = a \wedge b$. On écrit $a = da'$ et $b = db'$. Montrez que $a' \wedge b' = 1$ et que $a \vee b = da'b'$.
2. Déterminez tous les couples (a, b) d'entiers naturels tels que $a \wedge b = 12$ et $a \vee b = 360$.
3. Déterminez tous les couples (a, b) d'entiers naturels non nuls tels que $a + b = 84$ et $a \wedge b = 12$.

Exercice 11 : Test de primalité

1. Soit $n \geq 2$ un entier composé. Rappelez pourquoi n admet un diviseur premier p tel que $p^2 \leq n$.
2. L'entier 223 est-il premier ? Justifiez en limitant les essais.
3. Décomposez 221 et 391 en produit de nombres premiers.

Exercice 12 : Décomposition en facteurs premiers de 2520 et 3780

1. Décomposez 2520 et 3780 en produit de facteurs premiers.
2. En déduire $2520 \wedge 3780$ et $2520 \vee 3780$. Vérifiez la relation entre PGCD, PPCM et produit.
3. Combien 2520 possède-t-il de diviseurs positifs ?

Exercice 13 : Carrés parfaits et irrationalité

1. Montrez qu'un entier $n \geq 2$ est le carré d'un entier si et seulement si tous les exposants de sa décomposition en facteurs premiers sont pairs.
2. Déterminez le plus petit entier $k \geq 1$ tel que $2520k$ soit un carré parfait, et calculez la racine carrée obtenue.
3. En utilisant les valuations 2-adiques, démontrez que $\sqrt{6}$ est irrationnel.

Exercice 14 : Valuation p-adique de n! et zéros de 100!

Soit p un nombre premier et $n \geq 1$. On note $\lfloor x \rfloor$ la partie entière du réel x .

1. Montrez que le nombre de multiples de p^j compris entre 1 et n vaut $\lfloor n / p^j \rfloor$.
2. En déduire la formule de Legendre :
$$v_p(n!) = \sum_{j \geq 1} \lfloor n / p^j \rfloor.$$
3. Calculez $v_2(100!)$ et $v_5(100!)$.
4. Par combien de zéros l'écriture décimale de $100!$ se termine-t-elle ?

Exercice 15 : Calcul de restes par congruences

1. Déterminez le reste de la division euclidienne de 3^{100} par 7 .
2. Déterminez le reste de 2^{2026} modulo 9 .
3. Quel est le chiffre des unités de 7^{2026} ?
4. Montrez que pour tout $n \in \mathbb{N}$, 7 divise $2^{3n} - 1$.

Exercice 16 : Critères de divisibilité par 9 et par 11

Soit N un entier naturel d'écriture décimale $N = \sum_{k=0}^m c_k 10^k$, avec $c_k \in \{0, \dots, 9\}$.

1. Montrez que $N \equiv \sum_{k=0}^m c_k \pmod{9}$.
2. Montrez que $N \equiv \sum_{k=0}^m (-1)^k c_k \pmod{11}$.
3. L'entier 123456789 est-il divisible par 9 ? par 11 ? Donnez ses restes modulo 9 et 11 .
4. Montrez que 918082 est divisible par 11 .
5. Trouvez le chiffre x tel que le nombre $\overline{7x36}$ soit divisible par 9 .

Exercice 17 : Équations de congruence

1. Vérifiez que 19 est un inverse de 17 modulo 23 , puis résolvez $17x \equiv 5 \pmod{23}$.

2. Résolvez $6x \equiv 4 \pmod{10}$.

3. Montrez que $6x \equiv 3 \pmod{10}$ n'a pas de solution.

4. Énoncez une condition nécessaire et suffisante sur a , c et n pour que $ax \equiv c \pmod{n}$ ait une solution.

Exercice 18 : Système de congruences

On cherche les entiers x tels que

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 2 \pmod{7} \end{cases}$$

1. Montrez que les deux conditions $x \equiv 2 \pmod{3}$ et $x \equiv 2 \pmod{7}$ équivalent à $x \equiv 2 \pmod{21}$.

2. Écrivez $x = 2 + 21k$ et déterminez la condition sur k imposée par $x \equiv 3 \pmod{5}$.

3. En déduire toutes les solutions, ainsi que la plus petite solution positive.

Exercice 19 : Divisibilité de $n^7 - n$ par 42

1. À l'aide du petit théorème de Fermat, montrez que 7 divise $n^7 - n$ pour tout entier n .

2. Montrez que $n^7 - n$ est divisible par 2 et par 3.

3. En déduire que 42 divise $n^7 - n$ pour tout entier n .

Exercice 20 : Une démonstration du petit théorème de Fermat

Soit p un nombre premier.

1. Montrez que pour $1 \leq k \leq p-1$, p divise $\binom{p}{k}$.
2. En déduire que $(a+1)^p \equiv a^p + 1 \pmod{p}$ pour tout entier a .
3. Démontrez que $a^p \equiv a \pmod{p}$ pour tout $a \in \mathbb{N}$, puis pour tout $a \in \mathbb{Z}$.
4. En déduire que $a^{p-1} \equiv 1 \pmod{p}$ si p ne divise pas a .
5. Vérifiez que $2^{10} \equiv 1 \pmod{341}$. En déduire que $2^{340} \equiv 1 \pmod{341}$, puis que la réciproque du petit théorème de Fermat est fausse.

Exercice 21 : Infinité des nombres premiers de la forme $4k+3$

1. Montrez qu'un nombre premier impair est congru à 1 ou à 3 modulo 4 .
2. Montrez qu'un produit d'entiers tous congrus à 1 modulo 4 est congru à 1 modulo 4 .
3. On suppose qu'il n'existe qu'un nombre fini de nombres premiers congrus à 3 modulo 4 , notés $p_1, \dots, p_k$. On pose $N = 4p_1 p_2 \dots p_k - 1$. Montrez que N possède un diviseur premier congru à 3 modulo 4 .
4. Conclure.

Exercice 22 : PGCD des nombres de Mersenne

Pour $n \in \mathbb{N}^*$, on pose $M_n = 2^n - 1$.

1. Montrez que si d divise n , alors M_d divise M_n .
2. En déduire que si M_n est premier, alors n est premier. La réciproque est-elle vraie ? On pourra étudier M_{11} et le diviseur 23 .
3. Soient $a, b \in \mathbb{N}^*$ et $a = bq + r$ la division euclidienne de a par b . Montrez que $M_a = 2^r(2^{bq} - 1) + M_r$, avec la convention $M_0 = 0$, puis que $M_a \wedge M_b = M_b \wedge M_r$.
4. En déduire que $M_a \wedge M_b = M_{a \wedge b}$.
5. Calculez $M_{12} \wedge M_{18}$.

Exercice 23 : Problème, un chiffrement RSA miniature

On choisit les nombres premiers $p = 5$ et $q = 11$, et l'on pose $n = pq = 55$ et $m = (p - 1)(q - 1) = 40$. On choisit enfin $e = 3$. Un message est un entier x avec $0 \leq x \leq 54$. Le message chiffré est le reste de x^e modulo 55 .

1. Justifiez que $e \wedge m = 1$, puis trouvez l'unique entier d avec $1 \leq d \leq 39$ tel que $ed \equiv 1 \pmod{40}$.
2. Chiffrez le message $x = 2$, puis le message $x = 7$.
3. Soit $x \in \mathbb{Z}$. Montrez que $x^{ed} \equiv x \pmod{5}$, en distinguant selon que 5 divise x ou non.
4. Montrez de même que $x^{ed} \equiv x \pmod{11}$.

5. En déduire que $x^{ed} \equiv x \pmod{55}$ pour tout entier x . Expliquez pourquoi élever le message chiffré à la puissance d permet de le déchiffrer.
6. Sans calculatrice, déchiffrez le message 13 en calculant le reste de 13^d modulo 5 puis modulo 11.

Le corrigé des exercices

Chaque exercice est corrigé en détail, question par question, sur la page suivante.



Pour aller plus loin en L1

- Le cours : [arithmétique dans \$\mathbb{Z}\$, cours de maths en L1](#)
- À maîtriser avant : [Entiers naturels, récurrence et dénombrement](#)
- Chapitre précédent : [Fonctions usuelles et fonctions réciproques](#)
- Chapitre suivant : [Polynômes et fractions rationnelles](#)
- Tester vos connaissances : [QCM de maths en L1 par chapitre](#)
- Le sommaire : [tous les chapitres de maths de L1](#) et la [licence de maths de L1 à L3](#)