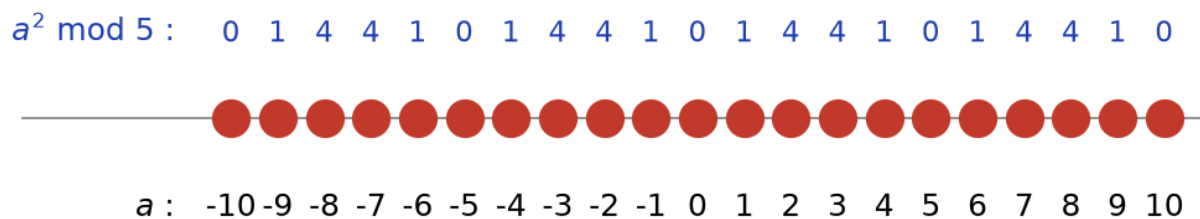


Arithmétique et $\mathbb{Z}/n\mathbb{Z}$

Exercice 1 : Relations d'équivalence et classes

La figure ci-dessous donne, pour chaque entier a de -10 à 10 , le reste de a^2 dans la division par 5 .



1. Sur $\mathbb{Z}$, on pose $a \mathcal{R} b \Leftrightarrow 5 \mid a^2 - b^2$. Montrez que $\mathcal{R}$ est une relation d'équivalence.
2. Montrez que $a \mathcal{R} b$ équivaut à $a \equiv b \pmod{5}$ ou $a \equiv -b \pmod{5}$. Décrivez toutes les classes et donnez le cardinal de $\mathbb{Z}/\mathcal{R}$.
3. Sur $\mathbb{Z}$, on pose $a \mathcal{S} b \Leftrightarrow a \mid b$ et $a \mathcal{T} b \Leftrightarrow |a - b| \leq 1$. Pour chacune, indiquez quelles propriétés d'une relation d'équivalence sont vérifiées, avec un contre-exemple pour les autres.
4. Sur $\mathbb{R}$, on pose $x \sim y \Leftrightarrow x - y \in \mathbb{Z}$. Montrez que chaque classe contient un unique élément de $[0, 1[$.

Exercice 2 : Congruences et critères de divisibilité

1. Montrez qu'un entier naturel est congru à la somme de ses chiffres modulo 9. Déduisez-en le reste de 123456789 modulo 9.
2. Montrez qu'un entier naturel $\overline{a_k \dots a_1 a_0}$ (écriture décimale) est congru modulo 11 à $a_0 - a_1 + a_2 - \dots + (-1)^k a_k$. Déduisez-en le reste de 123456789 modulo 11.
3. Déterminez le reste de 2026^{2026} dans la division par 9.
4. Vérifiez que $1001 = 7 \times 11 \times 13$, puis que $1000 \equiv -1$ modulo 7, 11 et 13. Déduisez-en les restes de 123456 modulo 7 et modulo 13.

Exercice 3 : Calculs dans $\mathbb{Z}/12\mathbb{Z}$

1. Déterminez les éléments inversibles de $\mathbb{Z}/12\mathbb{Z}$ et leurs inverses.
2. Montrez que chaque classe non nulle et non inversible est un diviseur de zéro, en exhibant pour chacune une classe non nulle qui l'annule.
3. Résolvez dans $\mathbb{Z}/12\mathbb{Z}$ l'équation $\bar{5}x + \bar{3} = \bar{10}$.
4. Résolvez $\bar{4}x = \bar{8}$, puis $\bar{4}x = \bar{6}$.
5. Calculez $\bar{7}^{100}$ et $\bar{5}^{2027}$.

Exercice 4 : Opérations bien définies sur le quotient

Pour $k \geq 1$ et $x \in \mathbb{Z}$, on note $\bar{x}^{(k)}$ la classe de x modulo k .

1. Soient $a \equiv a'$ et $b \equiv b'$ modulo n . Montrez directement que $ab \equiv a'b' \pmod{n}$.
2. Expliquez pourquoi la formule $f(\bar{x}) = \overline{2^x}$, pour $x \in \mathbb{N}$, ne définit pas une application de $\mathbb{Z}/3\mathbb{Z}$ dans $\mathbb{Z}/3\mathbb{Z}$. Montrez en revanche que $\overline{2^x}^{(3)}$ ne dépend que de la classe de x modulo 2.
3. Montrez que $\bar{x}^{(6)} \rightarrow \bar{x}^{(3)}$ définit un morphisme d'anneaux surjectif de $\mathbb{Z}/6\mathbb{Z}$ sur $\mathbb{Z}/3\mathbb{Z}$, et déterminez son noyau.
4. Montrez que $\bar{x}^{(3)} \rightarrow \bar{x}^{(6)}$ n'est pas bien définie.
5. Soient $m, n \geq 1$. Montrez que $\bar{x}^{(n)} \rightarrow \bar{x}^{(m)}$ est bien définie si et seulement si $m \mid n$.

Exercice 5 : Inverse d'une classe par Bézout

1. Justifiez que $\overline{17}$ est inversible dans $\mathbb{Z}/60\mathbb{Z}$ et calculez son inverse par l'algorithme d'Euclide étendu.
2. Résolvez $17x \equiv 5 \pmod{60}$.
3. Calculez l'inverse de $\overline{23}$ dans $\mathbb{Z}/101\mathbb{Z}$, puis résolvez $23x \equiv 7 \pmod{101}$.
4. La classe $\overline{21}$ est-elle inversible dans $\mathbb{Z}/60\mathbb{Z}$? Justifiez.

Exercice 6 : Équations linéaires modulo n

1. Soient $a, b \in \mathbb{Z}$, $n \geq 1$ et $d = \text{pgcd}(a, n)$. Montrez que $ax \equiv b \pmod{n}$ a des solutions si et seulement si $d \mid b$, et qu'il y a alors exactement d solutions modulo n .
2. Résolvez $6x \equiv 9 \pmod{15}$.
3. Résolvez $6x \equiv 10 \pmod{15}$.
4. Résolvez $14x \equiv 21 \pmod{35}$.

Exercice 7 : $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier

Soit $n \geq 2$.

1. Montrez que si n n'est pas premier, $\mathbb{Z}/n\mathbb{Z}$ n'est pas intègre, donc n'est pas un corps.
2. Montrez que si $n = p$ est premier, $\mathbb{Z}/p\mathbb{Z}$ est un corps.
3. Soit p premier. Montrez que les seules solutions de $x^2 = \bar{1}$ dans $\mathbb{Z}/p\mathbb{Z}$ sont $\bar{1}$ et $-\bar{1}$.
4. Dédisez-en le théorème de Wilson : $(p-1)! \equiv -1 \pmod{p}$. On pourra regrouper chaque facteur avec son inverse.
5. Calculez $10!$ modulo 11 , puis $9!$ modulo 11 , sans calculer ces factorielles.
6. Montrez que si $n \geq 2$ n'est pas premier, alors $(n-1)! \not\equiv -1 \pmod{n}$.

Exercice 8 : Calculs d'indicatrice d'Euler

1. Calculez $\varphi(97)$, $\varphi(1024)$, $\varphi(100)$ et $\varphi(360)$.
2. Montrez que $\varphi(n)$ est pair pour tout $n \geq 3$.
3. Déterminez tous les entiers $n \geq 1$ tels que $\varphi(n) = 4$.

Exercice 9 : Somme des indicatrices des diviseurs

Soit $n \geq 1$. On veut montrer que $\sum_{d|n} \varphi(d) = n$, la somme portant sur les diviseurs positifs de n .

1. Vérifiez la formule pour $n = 12$.
2. Vérifiez-la pour $n = p^k$, avec p premier et $k \geq 1$.
3. Pour $d|n$, on pose $A_d = \{k \in \{1, \dots, n\} \mid \text{pgcd}(k, n) = n/d\}$. Montrez que $k \rightarrow kd/n$ est une bijection de A_d sur $\{j \in \{1, \dots, d\} \mid \text{pgcd}(j, d) = 1\}$.
4. Concluez.

Exercice 10 : Exponentiation rapide

1. Écrivez 45 en base 2 . Calculez 3^{45} modulo 23 par la méthode des carrés successifs, puis vérifiez le résultat avec le petit théorème de Fermat.
2. Calculez 3^{100} modulo 7 et 2^{1000} modulo 13 .
3. Déterminez les deux derniers chiffres de 7^{2026} .
4. Calculez 5^{117} modulo 19 .

Exercice 11 : Petit théorème de Fermat et divisibilité

1. Montrez que pour tout $n \in \mathbb{Z}$, 42 divise $n^7 - n$.
2. Déterminez le reste de 2026^{2026} dans la division par 11 .
3. Montrez que $2^{340} \equiv 1 \pmod{341}$. Qu'en déduisez-vous sur la réciproque du petit théorème de Fermat ?

4. Soit p premier. Montrez que $(a + b)^p \equiv a^p + b^p \pmod{p}$ pour tous $a, b \in \mathbb{Z}$.

Exercice 12 : Théorème d'Euler et derniers chiffres

1. Calculez $\varphi(1000)$. Déduisez-en les trois derniers chiffres de 3^{2026} .
2. Déterminez le chiffre des unités de 7^{7^7} .
3. Montrez que pour tout entier a premier avec 10, $a^{20} \equiv 1 \pmod{100}$. Pourquoi l'exposant $\varphi(100) = 40$ n'est-il pas optimal ici ?

Exercice 13 : Système de congruences à modules premiers entre eux

1. Résolvez le système $x \equiv 2 \pmod{3}$, $x \equiv 3 \pmod{5}$, $x \equiv 2 \pmod{7}$ par la méthode des coefficients de Bézout.
2. Retrouvez le résultat en fusionnant les équations deux par deux.
3. Un groupe compte entre 200 et 300 personnes. Rangées par 3, il en reste 2 ; par 5, il en reste 3 ; par 7, il en reste 2. Combien sont-elles ?

Exercice 14 : Système de congruences à modules non premiers entre eux

1. Soient $m, n \geq 1$ et $d = \text{pgcd}(m, n)$. Montrez que le système $x \equiv a \pmod{m}$, $x \equiv b \pmod{n}$ a une solution si et seulement si $a \equiv b \pmod{d}$.
2. Montrez que deux solutions sont congrues modulo $\text{ppcm}(m, n)$.
3. Résolvez $x \equiv 5 \pmod{12}$, $x \equiv 11 \pmod{18}$.

4. Le système $x \equiv 1 \pmod{6}$, $x \equiv 2 \pmod{4}$ a-t-il des solutions ?

Exercice 15 : Isomorphisme chinois dans $\mathbb{Z}/15\mathbb{Z}$

On note $\psi : \mathbb{Z}/15\mathbb{Z} \rightarrow \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ l'application $x \bmod 15 \rightarrow (x \bmod 3, x \bmod 5)$.

1. Justifiez que ψ est un isomorphisme d'anneaux.
2. Déterminez l'antécédent de $(\bar{2}, \bar{4})$.
3. Retrouvez $\varphi(15)$ à l'aide de ψ et listez les inversibles de $\mathbb{Z}/15\mathbb{Z}$.
4. Résolvez $x^2 = \bar{1}$ dans $\mathbb{Z}/15\mathbb{Z}$. Comparez avec le cas d'un corps.
5. Résolvez $x^2 = x$ dans $\mathbb{Z}/15\mathbb{Z}$.

Exercice 16 : Carrés dans $\mathbb{F}_{11}$

1. Dressez la liste des carrés de $\mathbb{F}_{11}$. Combien y a-t-il de carrés non nuls ?
2. Vérifiez le critère d'Euler pour $a = 3$ et pour $a = 2$.
3. Résolvez $x^2 = \bar{5}$ dans $\mathbb{F}_{11}$.
4. Résolvez $x^2 + x - 1 = 0$, puis $x^2 + x + 1 = 0$ dans $\mathbb{F}_{11}$.

Exercice 17 : Critère d'Euler et produit de non-carrés

Soit p un nombre premier impair. On note C l'ensemble des carrés de $\mathbb{F}_p^\times$.

1. Montrez que C est un sous-groupe de $\mathbb{F}_p^\times$ de cardinal $\frac{p-1}{2}$.
2. Démontrez le critère d'Euler : pour $a \in \mathbb{F}_p^\times$, $a \in C \Leftrightarrow a^{\frac{p-1}{2}} = 1$, et sinon $a^{\frac{p-1}{2}} = -1$.
3. Déduisez-en que le produit de deux non-carrés est un carré, et que le produit d'un carré par un non-carré n'est pas un carré.
4. Dans $\mathbb{F}_7$, déterminez si 2, 3 et 6 sont des carrés, puis illustrez la question 3.

Exercice 18 : -1 est-il un carré modulo p ?

Soit p un nombre premier impair.

1. Montrez que -1 est un carré dans $\mathbb{F}_p$ si et seulement si $p \equiv 1 \pmod{4}$.
2. On pose $A = \left(\frac{p-1}{2}\right)!$. En associant k et $p-k$ dans $(p-1)!$, montrez que $A^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}$.
3. Déduisez-en une racine carrée explicite de -1 modulo p lorsque $p \equiv 1 \pmod{4}$. Calculez-la pour $p = 13$.
4. Montrez qu'il existe une infinité de nombres premiers congrus à 1 modulo 4. On pourra considérer $N = (2 p_1 \dots p_r)^2 + 1$.

Exercice 19 : Un chiffrement RSA à la main

Un destinataire choisit $p = 5$, $q = 11$ et $e = 3$.

1. Calculez n et $\varphi(n)$, et vérifiez que e convient.
2. Calculez la clé privée d .
3. Chiffrez les messages $m = 2$ et $m = 7$.
4. Déchiffrez $c = 13$ en calculant 13^{27} modulo 5 et modulo 11 , puis en appliquant le théorème chinois.
5. Expliquez pourquoi la connaissance de p et q permet de casser ce chiffrement.

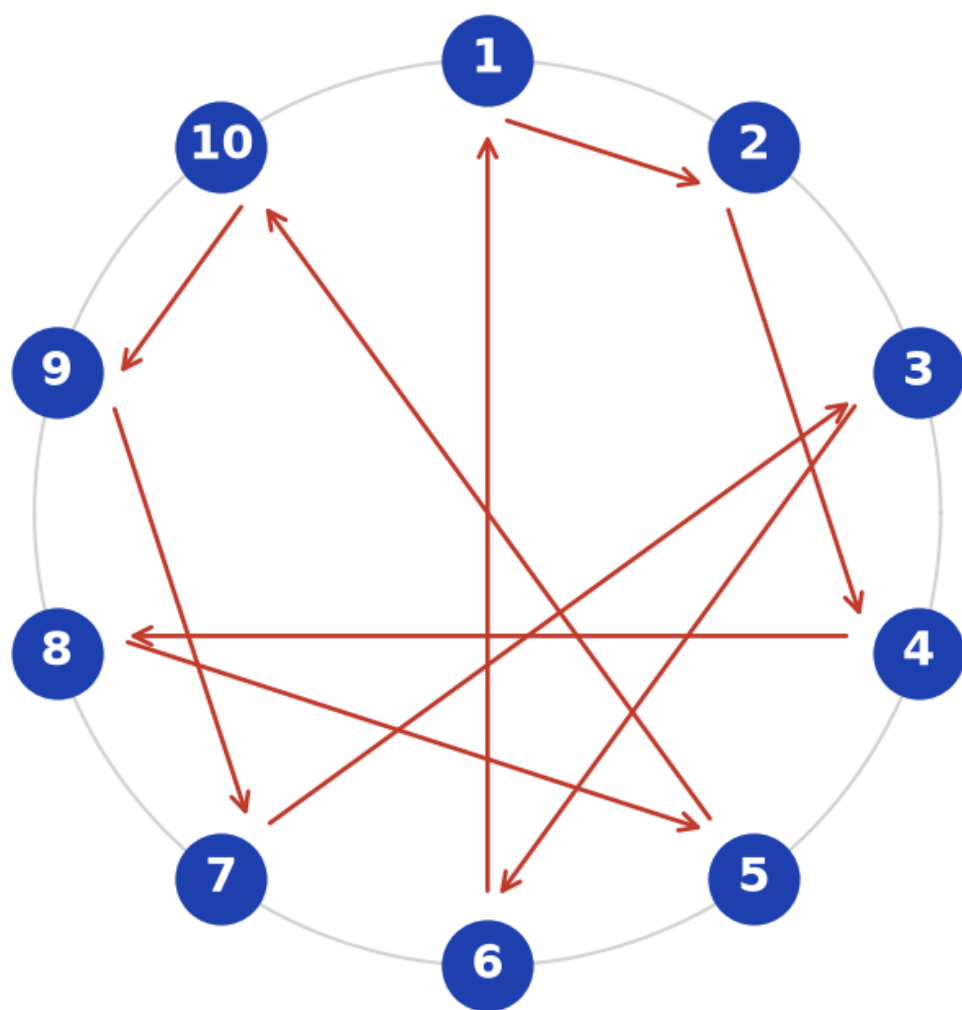
Exercice 20 : Correction du RSA et factorisation

Soient $p \neq q$ deux nombres premiers, $n = pq$, e premier avec $\varphi(n)$ et d tel que $ed \equiv 1 \pmod{\varphi(n)}$.

1. Montrez que $m^{ed} \equiv m \pmod{n}$ pour tout $m \in \mathbb{Z}$, y compris lorsque m n'est pas premier avec n .
2. Dédisez-en que $x \rightarrow x^e$ est une bijection de $\mathbb{Z}/n\mathbb{Z}$ dans lui-même, et donnez sa réciproque.
3. On sait que $n = 391$ et $\varphi(n) = 352$. Retrouvez p et q .
4. Avec $n = 391$ et $e = 3$, vérifiez que e convient et calculez d .

Exercice 21 : Problème : ordre multiplicatif et nombres de Carmichael

Soient $n \geq 2$ et a un entier premier avec n . La figure ci-dessous représente l'application $x \rightarrow ax$ sur les classes non nulles de $\mathbb{Z}/n\mathbb{Z}$.



flèche : $x \mapsto 2x$ dans $\mathbb{Z}/11\mathbb{Z}$

1. Montrez que l'ensemble $\{k \geq 1 \mid a^k \equiv 1, 1 \pmod{n}\}$ est non vide. On note $\omega(a)$ son plus petit élément, appelé ordre de a modulo n .
2. Montrez que $a^k \equiv 1 \pmod{n}$ si et seulement si $\omega(a) \mid k$. Déduisez-en que $\omega(a)$ divise $\varphi(n)$.
3. Déterminez l'ordre de 2 modulo 11 en n'effectuant que trois calculs. Que lit-on sur la figure ?
4. Déterminez l'ordre de 3 modulo 11.
5. Soit $p \notin \{2, 5\}$ premier. Montrez que la période du développement décimal de $1/p$ est l'ordre de 10 modulo p . Vérifiez-le pour $p = 7$ et $p = 13$.

6. On considère $561 = 3 \times 11 \times 17$. Montrez que $a^{560} \equiv 1 \pmod{561}$ pour tout a premier avec 561 .
7. Que peut-on en conclure sur le test « $a^{n-1} \equiv 1 \pmod{n}$ » comme test de primalité ?

Le corrigé des exercices

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



Pour aller plus loin en L2

- Le cours : [arithmétique et \$\mathbb{Z}/n\mathbb{Z}\$, cours de maths en L2](#)
- Chapitre précédent : [Polynômes d'endomorphismes et trigonalisation](#)
- Chapitre suivant : [Groupes, sous-groupes et morphismes](#)
- Tester vos connaissances : [QCM de maths en L2 par chapitre](#)
- Le sommaire : [tous les chapitres de maths de L2](#) et la [licence de maths de L1 à L3](#)