

Arithmétique dans $\mathbb{Z}$

Exercice 1 : Division euclidienne et carrés modulo 8

Cet exercice revient aux définitions. Il prépare aussi les raisonnements par disjonction des restes.

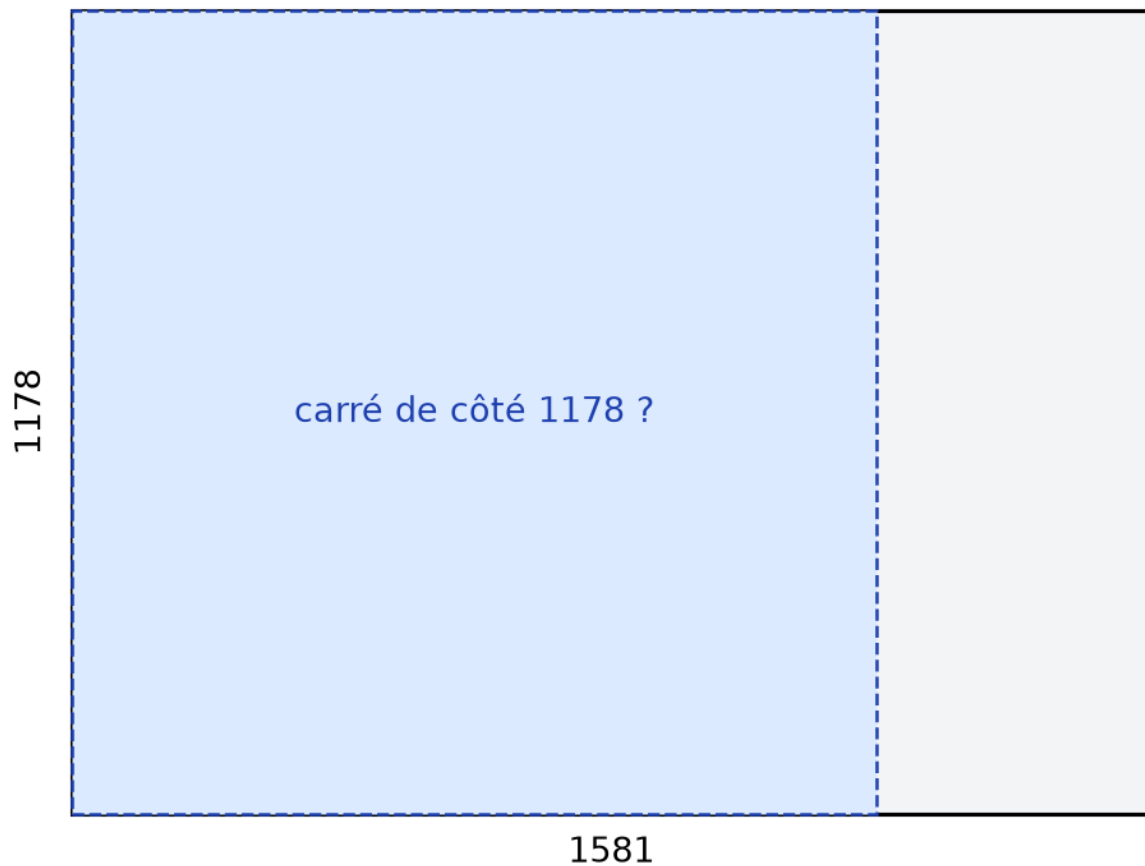
1. Effectuez la division euclidienne de 2026 par 37, puis celle de -250 par 13.
2. Soit $n \in \mathbb{Z}$. Déterminez les restes possibles de n^2 dans la division euclidienne par 8. En particulier, montrez que le carré d'un entier impair a pour reste 1.
3. Dédisez-en qu'aucun entier de reste 7 dans la division par 8 n'est somme de trois carrés d'entiers.

Exercice 2 : Divisibilité par récurrence

1. Montrez que, pour tout $n \in \mathbb{N}$, l'entier $3^{2n+1} + 2^{n+2}$ est divisible par 7.
2. Montrez que, pour tout $n \in \mathbb{N}$, l'entier $4^n + 6n - 1$ est divisible par 9.

Exercice 3 : PGCD par l'algorithme d'Euclide

On considère un rectangle de côtés 1581 et 1178. On le découpe en carrés : d'abord le plus grand carré possible, puis on recommence dans le rectangle restant, comme le suggère la figure ci-dessous.



1. Soient $a, b, q, r \in \mathbb{Z}$ tels que $a = bq + r$. Montrez que $a \wedge b = b \wedge r$.
2. Calculez $1581 \wedge 1178$ par l'algorithme d'Euclide. Quel est le côté du dernier carré du découpage ?
3. Déduisez-en $1581 \vee 1178$.

Exercice 4 : Algorithme d'Euclide étendu

1. À l'aide de l'algorithme d'Euclide étendu, déterminez un couple $(u, v) \in \mathbb{Z}^2$ tel que $2026u + 311v = 1$.
2. Déduisez-en un inverse de 311 modulo 2026, compris entre 0 et 2025.
3. Résolvez la congruence $311x \equiv 2 \pmod{2026}$.

Exercice 5 : Existence de solutions de $ax + by = c$

On étudie l'équation $12x + 18y = c$, d'inconnue $(x, y) \in \mathbb{Z}^2$, où $c \in \mathbb{Z}$.

1. Montrez que l'équation admet une solution si et seulement si 6 divise c .
2. Résolvez $12x + 18y = 30$.
3. L'équation $12x + 18y = 25$ a-t-elle des solutions ?

Exercice 6 : Équation diophantienne $17x + 23y = c$

1. Justifiez que $17 \wedge 23 = 1$, puis trouvez un couple (u, v) tel que $17u + 23v = 1$.
2. Résolvez dans $\mathbb{Z}^2$ l'équation $17x + 23y = 5$. Existe-t-il une solution avec $x \geq 0$ et $y \geq 0$?
3. Déterminez tous les couples d'entiers naturels (x, y) tels que $17x + 23y = 500$.
4. Interprétation : un distributeur rend des pièces de 17 et de 23 unités. De combien de façons peut-il rendre exactement 500 unités ?

Exercice 7 : PGCD d'expressions polynomiales en n

Dans tout l'exercice, n désigne un entier naturel.

1. Montrez que $2n + 3$ et $3n + 4$ sont premiers entre eux.
2. Calculez $(n^2 + 1) \wedge (n + 1)$ selon la parité de n .

- Montrez que $n \wedge (2n + 1) = 1$, puis que $(n^3 + n) \wedge (2n + 1) = (n^2 + 1) \wedge (2n + 1)$.
- Montrez que $(n^2 + 1) \wedge (2n + 1)$ divise 5. Déterminez les n pour lesquels $(n^3 + n) \wedge (2n + 1) = 5$.

Exercice 8 : Couples d'entiers de PGCD et PPCM donnés

- Soient $a, b \in \mathbb{N}^*$, $d = a \wedge b$, $a = da'$ et $b = db'$. Montrez que $a \vee b = da'b'$, en utilisant le lemme de Gauss. Dédisez-en que $(a \wedge b)(a \vee b) = ab$.
- Déterminez tous les couples (a, b) d'entiers naturels, avec $a \leq b$, tels que $a \wedge b = 18$ et $a \vee b = 540$.
- Déterminez tous les couples (a, b) d'entiers naturels, avec $a \leq b$, tels que $a + b = 360$ et $a \wedge b = 45$.

Exercice 9 : Racines rationnelles et lemme de Gauss

Soit $P = a_n X^n + \dots + a_1 X + a_0$ un polynôme à coefficients entiers, avec $a_n \neq 0$ et $a_0 \neq 0$.

- Soit $\frac{p}{q}$ une racine rationnelle de P , écrite sous forme irréductible avec $q \geq 1$. Montrez que p divise a_0 et que q divise a_n .
- Déterminez les racines rationnelles de $6X^3 - 11X^2 + 6X - 1$, puis factorisez ce polynôme.
- Montrez que $\sqrt[3]{2}$ est irrationnel.

Exercice 10 : PGCD de trois entiers

1. Calculez $330 \wedge 462 \wedge 770$, puis trouvez des entiers u, v, w tels que $330u + 462v + 770w = 330 \wedge 462 \wedge 770$.
2. Montrez que $6, 10, 15$ sont premiers entre eux dans leur ensemble, mais pas deux à deux. Trouvez $u, v, w \in \mathbb{Z}$ tels que $6u + 10v + 15w = 1$.
3. Soient $a_1, \dots, a_n$ des entiers premiers entre eux deux à deux, qui divisent tous un entier N . Montrez par récurrence que $a_1 a_2 \dots a_n$ divise N .
4. Déterminez le plus petit entier naturel non nul divisible par $4, 9$ et 25 . Le résultat reste-t-il vrai avec $4, 6$ et 25 ?

Exercice 11 : Crible d'Ératosthène jusqu'à 120

La grille ci-dessous contient les entiers de 1 à 120 .

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100
101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120

1. Soit $n \geq 2$ un entier non premier. Montrez que n admet un diviseur premier p tel que $p^2 \leq n$.
2. Appliquez le crible d'Ératosthène à la grille. Quels nombres premiers suffit-il d'utiliser ? Combien de nombres premiers inférieurs ou égaux à 120 obtenez-vous ?
3. Sans le crible, montrez que 113 est premier et que 119 ne l'est pas.

4. Soit $n \geq 2$. Montrez que les $n - 1$ entiers consécutifs $n! + 2, n! + 3, \dots, n! + n$ sont tous composés. Qu'en déduisez-vous sur les écarts entre nombres premiers ?

Exercice 12 : Infinité des premiers de la forme $6k + 5$

1. Montrez qu'un nombre premier $p \geq 5$ a pour reste 1 ou 5 dans la division par 6.
2. Montrez qu'un produit d'entiers de reste 1 modulo 6 a encore pour reste 1 modulo 6.
3. Soit $N \geq 2$ un entier de reste 5 modulo 6. Montrez que N possède un diviseur premier de reste 5 modulo 6.
4. On suppose qu'il n'existe qu'un nombre fini de nombres premiers de reste 5 modulo 6, notés $p_1, \dots, p_r$. En considérant $N = 6p_1p_2 \dots p_r - 1$, aboutissez à une contradiction.

Exercice 13 : Nombres de Fermat

Pour $n \in \mathbb{N}$, on pose $F_n = 2^{2^n} + 1$. Ainsi $F_0 = 3$, $F_1 = 5$, $F_2 = 17$ et $F_3 = 257$.

1. Montrez que, pour tout $n \geq 1$, $F_0 F_1 \dots F_{n-1} = F_n - 2$.
2. Déduisez-en que les nombres de Fermat sont premiers entre eux deux à deux.
3. En associant à chaque F_n l'un de ses diviseurs premiers, donnez une nouvelle preuve de l'infinité des nombres premiers.
4. On pose $p = 641$. Vérifiez que $p = 5 \times 2^7 + 1 = 5^4 + 2^4$. Déduisez-en, par des congruences modulo 641, que 641 divise F_5 . Les nombres de Fermat sont-ils tous premiers ?

Exercice 14 : Décomposition de 4200 et 1764

1. Décomposez 4200 et 1764 en produits de facteurs premiers.
2. Déduisez-en $4200 \wedge 1764$ et $4200 \vee 1764$, puis vérifiez la relation entre leur produit et 4200×1764 .
3. Combien 4200 possède-t-il de diviseurs positifs ?
4. Déterminez le plus petit entier $k \geq 1$ tel que $4200k$ soit un carré parfait, puis le plus petit tel que $4200k$ soit un cube parfait.

Exercice 15 : Formule de Legendre et zéros de 1000!

Pour x réel, $\lfloor x \rfloor$ désigne la partie entière de x .

1. Soient p premier et $n \in \mathbb{N}^*$. Montrez que le nombre de multiples de p^k compris entre 1 et n vaut $\lfloor n / p^k \rfloor$. Déduisez-en la formule de Legendre :

$$v_p(n!) = \sum_{k \geq 1} \left\lfloor \frac{n}{p^k} \right\rfloor.$$

2. Calculez $v_5(1000!)$ et $v_2(1000!)$. Par combien de zéros l'écriture décimale de $1000!$ se termine-t-elle ?
3. Calculez $v_7(1000!)$.
4. Déterminez les entiers n tels que $n!$ se termine par exactement six zéros. Existe-t-il un entier n tel que $n!$ se termine par exactement cinq zéros ?

Exercice 16 : Nombre et somme des diviseurs

Soit $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ la décomposition en facteurs premiers d'un entier $n \geq 2$. On note $d(n)$ le nombre de diviseurs positifs de n et $\sigma(n)$ leur somme.

1. Montrez que les diviseurs positifs de n sont les entiers $p_1^{\beta_1} \dots p_r^{\beta_r}$ avec $0 \leq \beta_i \leq \alpha_i$.
Déduisez-en $d(n) = (\alpha_1 + 1) \dots (\alpha_r + 1)$.
2. Montrez que $\sigma(n) = \prod_{i=1}^r \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}$. Calculez $d(360)$ et $\sigma(360)$.
3. Montrez que $d(n)$ est impair si et seulement si n est un carré parfait.
4. Déterminez le plus petit entier naturel possédant exactement 12 diviseurs positifs.

Exercice 17 : Critères de divisibilité et derniers chiffres

1. Soit $N = \sum_{k=0}^m c_k 10^k$ l'écriture décimale de N . Montrez que

$$N \equiv_{[9]} c_0 + c_1 + \dots + c_m \quad \text{et que} \quad N \equiv_{[11]} c_0 - c_1 + c_2 - \dots + (-1)^m c_m.$$
2. L'entier 918 273 645 est-il divisible par 9 ? Par 11 ? Donnez son reste modulo 11.
3. Montrez que $3^{20} \equiv_{[100]} 1$. Déduisez-en les deux derniers chiffres de 3^{2026} .
4. Déterminez le reste de 5^{2026} dans la division par 9.

Exercice 18 : Inverse modulo n et congruences linéaires

1. Soit $n \geq 2$. Montrez que a est inversible modulo n si et seulement si $a \wedge n = 1$. Listez les entiers de $\left\{ \begin{smallmatrix} 0, \\ fs4\dots, 11 \end{smallmatrix} \right\}$ inversibles modulo 12 et donnez leurs inverses.
2. Déterminez un inverse de 17 modulo 43, puis résolvez $17x \equiv_{[43]} 5$.
3. Résolvez $6x \equiv_{[10]} 4$.

4. Montrez que $6x \equiv 5 \pmod{10}$ n'a aucune solution.

Exercice 19 : Congruences simultanées

1. Déterminez les entiers x tels que $x \equiv 2 \pmod{5}$ et $x \equiv 3 \pmod{7}$.
2. Déterminez les entiers x vérifiant de plus $x \equiv 1 \pmod{3}$.
3. Une coopérative range ses œufs par boîtes de 3, de 5 ou de 7. Il reste alors respectivement 1, 2 et 3 œufs. Sachant qu'elle possède entre 100 et 200 œufs, combien en a-t-elle ?
4. Montrez que le système $x \equiv 1 \pmod{4}$ et $x \equiv 2 \pmod{6}$ n'a aucune solution. Quelle hypothèse manque par rapport aux questions précédentes ?

Exercice 20 : Petit théorème de Fermat et calculs de restes

1. Déterminez le reste de 2^{2026} dans la division par 13.
2. Déterminez le reste de 7^{1003} dans la division par 11.
3. À l'aide du petit théorème de Fermat, calculez un inverse de 5 modulo 13, puis résolvez $5x \equiv 3 \pmod{13}$.
4. Montrez que 13 divise $2^{70} + 3^{70}$.

Exercice 21 : Fermat et divisibilité par 2730

1. Soit p un nombre premier tel que $p - 1$ divise 12. Montrez que $n^{13} \equiv n \pmod{p}$ pour tout

$$n \in \mathbb{Z}.$$

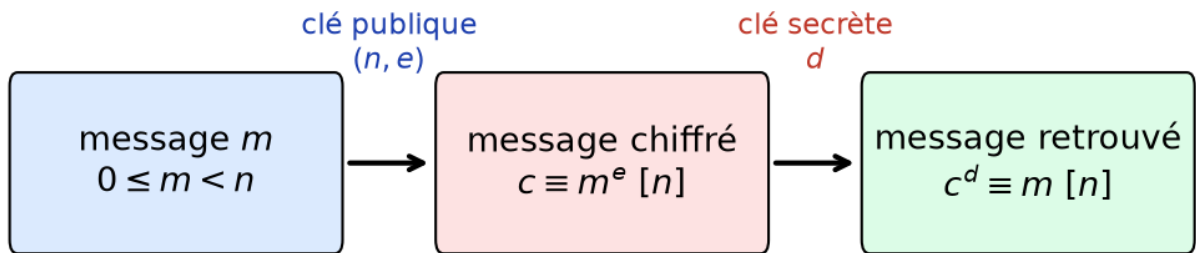
- Déduisez-en que 2730 divise $n^{13} - n$ pour tout entier n .
- Montrez que 15 divise $3n^5 + 5n^3 + 7n$ pour tout entier n .
- Soit p un nombre premier. Montrez que
$$1^{p-1} + 2^{p-1} + \dots + (p-1)^{p-1} \equiv -1 \pmod{p}.$$

Exercice 22 : Nombres de Mersenne et leurs diviseurs

- Soient $a \geq 2$ et $n \geq 2$. Montrez que si $a^n - 1$ est premier, alors $a = 2$ et n est premier.
- Soient $a, b \in \mathbb{N}^*$. En écrivant $a = bq + r$, montrez que
$$(2^a - 1) \wedge (2^b - 1) = (2^b - 1) \wedge (2^r - 1).$$
 Déduisez-en
$$(2^a - 1) \wedge (2^b - 1) = 2^{a \wedge b} - 1.$$
- Vérifiez que $2^{11} - 1 = 23 \times 89$. La réciproque de la question 1 est-elle vraie ?
- Soient p un nombre premier impair et q un diviseur premier de $2^p - 1$. Montrez que
$$q \equiv 1 \pmod{2p}.$$
- Déduisez-en que $2^{13} - 1 = 8191$ est premier en testant au plus deux divisions.

Exercice 23 : Problème : principe du chiffrement RSA

Le chiffrement RSA utilise deux nombres premiers distincts p et q , et $n = pq$. On choisit $e \geq 1$ premier avec $(p-1)(q-1)$, et $d \geq 1$ tel que
$$ed \equiv 1 \pmod{(p-1)(q-1)}.$$
 Le schéma ci-dessous résume le principe.



$n = pq$ connu de tous ; p , q et d gardés secrets

1. On prend $p = 5$, $q = 11$ et $e = 3$. Calculez n et $(p-1)(q-1)$, vérifiez que e convient et déterminez le plus petit $d \geq 1$ possible.
2. Revenons au cas général. Justifiez qu'il existe $k \in \mathbb{N}$ tel que $ed = 1 + k(p-1)(q-1)$. Montrez alors que $m^{ed} \equiv m \pmod{p}$ pour tout $m \in \mathbb{Z}$, en distinguant deux cas.
3. Déduisez-en que $m^{ed} \equiv m \pmod{n}$ pour tout $m \in \mathbb{Z}$.
4. Avec les valeurs de la question 1, chiffrez le message $m = 8$, c'est-à-dire calculez le reste c de m^e modulo 55.
5. Déchiffrez c : calculez les restes de c^d modulo 5 et modulo 11, puis retrouvez m .
6. Expliquez pourquoi la connaissance de p et q permet de retrouver d à partir de (n, e) .

Le corrigé des exercices

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

Pour aller plus loin en maths sup

- Le cours : [arithmétique dans \$\mathbb{Z}\$, cours de maths sup](#)
- À maîtriser avant : [Logique, ensembles, applications et relations](#)
- Chapitre précédent : [Dérivabilité et convexité](#)
- Chapitre suivant : [Structures algébriques usuelles : groupes, anneaux, corps](#)
- Le même thème en L1 : [arithmétique dans \$\mathbb{Z}\$, exercices de maths en L1](#)
- Tester vos connaissances : [QCM de maths sup par chapitre](#)
- Le sommaire : [tous les chapitres de maths sup](#) et les [chapitres de maths spé](#)