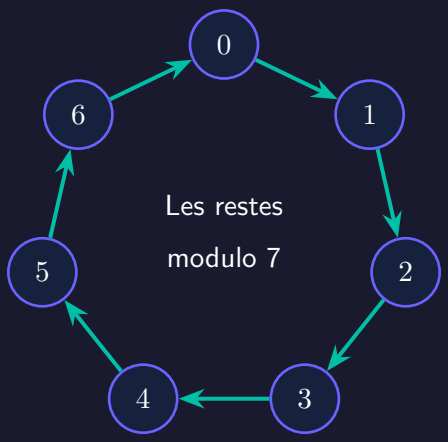
FICHE 04

Divisibilité et congruences

Divisibilité ▪ Division euclidienne ▪ Restes



Terminale — Option Mathématiques expertes — Programme officiel

Cours | 15 exercices | Problème guidé | Corrigés

Table des matières

1 Pourquoi ce chapitre ?

1.1 Le problème fondamental : résoudre dans les entiers

Pour partager 23 objets en lots de 5, le quotient réel 4,6 n'est pas le résultat attendu : tu obtiens 4 lots et 3 objets restants. En arithmétique, la contrainte entière change la question. Nous allons formaliser cette idée de reste, puis l'utiliser pour remplacer certains calculs immenses par quelques possibilités.

Intuition | Un calcul utile peut oublier de l'information

Pour connaître le jour de la semaine dans 100 jours, il suffit de connaître le reste de 100 dans la division par 7. Les 14 semaines complètes ne changent pas le jour. Oublier le quotient est ici une simplification volontaire, adaptée à la question posée.

Prérequis. Entiers relatifs, multiples, distributivité, puissances, division d'entiers positifs, preuve par contraposée ou par l'absurde. On note $\mathbb{N} = \{0, 1, 2, \ldots\}$ et $\mathbb{Z}$ l'ensemble des entiers relatifs.

Méthode | Objectifs

Passer d'une divisibilité à une égalité ; maîtriser la division euclidienne même avec un dividende négatif ; calculer modulo un entier ; prouver un test de divisibilité ; reconnaître les simplifications autorisées.

Le cours suit le socle officiel. Le problème de chiffrement affine est une application guidée ; la méthode générale pour inverser un entier modulo n sera démontrée dans la fiche 5.

Méthode | Comment travailler cette fiche

Commence par l'idée avant la formule, puis travaille une notion à la fois. Dans le cours, reformule la définition avec tes mots et refais l'exemple sans regarder la dernière ligne. Les pauses te proposent une question, deux indices graduels et une explication ; tu peux chercher avec une aide sans renoncer au raisonnement.
Après le cours, la boîte à outils relie plusieurs notions dans des méthodes commentées. Les exercices passent des bases aux questions d'initiative. Si tu bloques, prends d'abord un indice ; après le corrigé, explique pourquoi la méthode convient et refais une variante. Le problème final construit un approfondissement à partir du cours, puis une dernière activité te permet de faire le point.

2 L'idée avant la formule

2.1 Plusieurs entiers, un même reste

Les entiers 3, 10 et 17 ont le même reste modulo 7. Ils restent différents comme entiers, mais se comportent de la même manière si l'on ne regarde que le jour de la semaine. Leur différence est un multiple de 7 : c'est cette propriété exacte que la notation de congruence retiendra.

2.2 Un reste positif même en reculant

Reculer de 2 jours produit le même décalage qu'avancer de 5 jours. L'écriture $-2 = 7(-1) + 5$ possède un reste entre 0 et 6. Le quotient -1 compte un tour en arrière ; le reste 5 donne une position autorisée. Cette lecture évite de confondre le signe du nombre et celui du reste.

2.3 Détecter une impossibilité avant de chercher

Un carré entier est congru à 0 ou à 1 modulo 4. Une somme de deux carrés ne peut donc être congrue à 3. On pourra ainsi exclure une équation entière sans essayer tous les couples. Attention au sens logique : franchir un test modulaire ne garantit pas qu'une solution entière existe.

Méthode | Le fil de chaque raisonnement

Précise le module, remplace les nombres par des représentants simples, utilise une opération autorisée, puis retraduis le résultat dans la question de départ. Une congruence est un outil ; la conclusion doit parler du reste, de la divisibilité ou de l'équation demandée.

3 Le cours formel

3.1 Divisibilité dans les entiers relatifs

Définition | Diviseur et multiple

Pour $a, b \in \mathbb{Z}$, on écrit $a \mid b$ lorsqu'il existe $k \in \mathbb{Z}$ tel que $b = ak$. On dit que a divise b ou que b est un multiple de a.

Par exemple $-3 \mid 12$ car $12 = (-3)(-4)$. Tout entier divise 0 car $0 = a \times 0$. L'égalité $0 \mid b$ n'est vraie que pour $b = 0$. Pour un entier non nul b, ses diviseurs entiers viennent par paires opposées ; on précise « positifs » si l'on veut seulement ceux de $\mathbb{N}^*$.

Propriété | Règles fondamentales

Si $a \mid b$ et $b \mid c$, alors $a \mid c$. Si $d \mid a$ et $d \mid b$, alors $d \mid (ua + vb)$ pour tous $u, v \in \mathbb{Z}$. Pour $a, b \neq 0$, $a \mid b$ et $b \mid a$ impliquent $|a| = |b|$.

Démonstration | Revenir à l'égalité

Transitivité. Dire $a \mid b$ signifie qu'il existe un entier k tel que $b = ak$. Dire $b \mid c$ signifie qu'il existe un entier ℓ tel que $c = b\ell$. Remplaçons b dans cette seconde égalité : $c = (ak)\ell = a(k\ell)$. Comme le produit $k\ell$ est un entier, nous avons exhibé le quotient entier qui prouve $a \mid c$.
Combinaison linéaire. Si $d \mid a$ et $d \mid b$, écrivons $a = dr, b = ds$ avec $r, s \in \mathbb{Z}$. Alors $ua + vb = u(dr) + v(ds) = d(ur + vs)$. Si u, v sont entiers, $ur + vs$ est entier : c'est la condition nécessaire pour conclure à la divisibilité. La preuve reste valable pour des coefficients négatifs.
Divisibilité dans les deux sens. Si $a, b \neq 0$ et $b = ak$, alors $k \neq 0$. Un entier non nul a une valeur absolue au moins 1, donc $|b| = |a||k| \geq |a|$. L'hypothèse inverse $b \mid a$ donne de même $|a| \geq |b|$. Les deux inégalités imposent $|a| = |b|$. On ne conclut pas nécessairement $a = b$: les entiers opposés, par exemple 2 et -2, se divisent aussi mutuellement.

Exemple | Une combinaison utile

Nous cherchons à supprimer n pour obtenir une information sur d indépendante de n. Les coefficients de n sont 3 et 2 ; multiplions donc la première expression par 2 et la seconde par 3. Puisque d divise chacune, il divise leur différence :

$$3(2n + 1) - 2(3n + 1) = 6n + 3 - 6n - 2 = 1.$$

Ainsi $d \mid 1$, donc $1 = dk$ pour un entier k. Les seules possibilités sont $d = 1, k = 1$ ou $d = -1, k = -1$. Tous les diviseurs communs sont donc ± 1. Le choix des coefficients n'a pas été deviné sans raison : il visait les deux termes égaux $6n$.

Attention | Diviser n'est pas être plus petit

$2 \leq 3$ n'implique pas $2 \mid 3$. À l'inverse, un diviseur peut être négatif. Il faut produire un quotient entier, pas seulement un quotient réel.

À toi d'essayer : Transformer le symbole en égalité

Si d divise a et b, prouve qu'il divise $5a - 2b$. Pourquoi les coefficients entiers comptent-ils ?
Pour démarrer. Remplace chaque divisibilité par une égalité avec un quotient entier.

Tu peux chercher, prendre un indice ou lire l'explication, à ton rythme.

Indices, p. 27 Explication, p. 30

3.2 Division euclidienne : existence et unicité

Théorème | Division par un entier positif

Pour tout $a \in \mathbb{Z}$ et tout $b \in \mathbb{N}^*$, il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que

$$a = bq + r, \qquad 0 \leq r < b.$$

q est le quotient et r le reste. En particulier, $b \mid a$ équivaut à $r = 0$.

Démonstration | Pourquoi ce couple existe et est unique

Construire un couple. Le symbole $\lfloor x \rfloor$ désigne le plus grand entier inférieur ou égal à x. Par exemple $\lfloor 3{,}4 \rfloor = 3$ et $\lfloor -3{,}4 \rfloor = -4$. Choisissons $q = \lfloor a/b \rfloor$. Par définition, $q \leq a/b < q + 1$. Comme $b > 0$, multiplier conserve les sens : $bq \leq a < bq + b$. Soustraire bq donne $0 \leq a - bq < b$.
Posons $r = a - bq$. Il est entier puisque a, b, q le sont ; l'encadrement précédent dit qu'il est un reste autorisé. Sa définition donne aussi $a = bq + r$. Cela prouve l'existence.
Montrer qu'il ne peut y en avoir deux. Supposons $a = bq + r = bq' + r'$ avec $0 \leq r, r' < b$. En soustrayant, $b(q - q') = r' - r$. Comme les deux restes sont entre 0 et $b - 1$, leur différence est strictement entre $-b$ et b. Or les multiples de b les plus proches de zéro sont $-b, 0, b$; le seul dans cet intervalle ouvert est 0. Donc $b(q - q') = 0$. Puisque $b \neq 0$, $q = q'$, et l'égalité initiale impose alors $r = r'$. Les bornes du reste sont donc ce qui assure l'unicité.

Exemple | Dividende négatif

Nous cherchons un multiple de 5 situé juste en dessous de -23. Les multiples voisins sont $-25 = 5(-5)$ et $-20 = 5(-4)$. Puisque $-25 \leq -23 < -20$, le quotient est -5. Le reste est la distance entière depuis -25 : $-23 - (-25) = 2$. Donc $-23 = 5(-5) + 2$, avec $0 \leq 2 < 5$.
L'écriture $5(-4) - 3 = -23$ est vraie, mais le reste -3 est interdit. Descendre le quotient de -4 à -5 retire 5 au produit ; on doit donc ajouter 5 au reste, qui devient $-3 + 5 = 2$, pour conserver la même somme.

Méthode | Contrôle à deux conditions

Vérifie simultanément l'égalité $a = bq + r$ et les bornes $0 \leq r < b$. Une égalité seule ne suffit pas. Si un reste provisoire est négatif, diminue le quotient de 1 et ajoute b au reste.

À toi d'essayer : Corriger un reste

On écrit $-17 = 4(-4) - 1$. Trouve la division euclidienne correcte.
Pour démarrer. Diminue le quotient de 1 et compense en ajoutant 4 au reste.

Tu peux chercher, prendre un indice ou lire l'explication, à ton rythme.

Indices, p. 27 Explication, p. 30

3.3 Congruences : oublier le quotient, garder le reste

Définition | Congruence modulo n

Pour $n \geq 1$ et $a, b \in \mathbb{Z}$, on écrit $a \equiv b \pmod{n}$ lorsque $n \mid (a - b)$. Cette condition équivaut à l'égalité de leurs restes dans la division euclidienne par n.

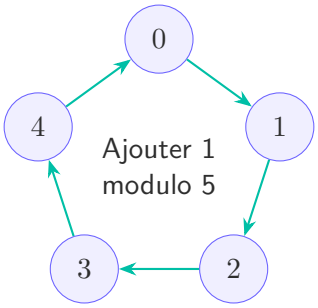
Démonstration | Équivalence avec les restes

Écrivons les divisions $a = nq + r$ et $b = nq' + r'$ avec $0 \leq r, r' < n$. La différence est $a - b = n(q - q') + (r - r')$.
Si les restes sont égaux, $r - r' = 0$, donc $a - b = n(q - q')$. Le quotient $q - q'$ est entier : $n \mid (a - b)$, c'est-à-dire $a \equiv b \pmod{n}$.
Si les nombres sont congrus, écrivons $a - b = nt$ avec $t \in \mathbb{Z}$. En comparant avec l'expression précédente, $r - r' = n[t - (q - q')]$ est un multiple de n. Mais $-n < r - r' < n$, puisque les deux restes sont autorisés. Le seul multiple possible est 0, donc $r = r'$. Nous avons démontré les deux sens de l'équivalence, pas seulement que des restes égaux suffisent.

Une congruence ne signifie pas une égalité : $17 \equiv 2 \pmod{5}$ mais $17 \neq 2$. Elle dépend du module : $17 \not\equiv 2 \pmod{4}$. Pour $n = 1$, tous les entiers sont congrus.

Propriété | Une relation cohérente

La congruence est réflexive ($a \equiv a$), symétrique et transitive. On peut remplacer un entier par un représentant plus simple, positif ou négatif : $10 \equiv -1 \pmod{11}$ est souvent plus utile que $10 \equiv 10 \pmod{11}$.



Chaque entier se place dans l'une des cinq classes de restes. Après 4, ajouter 1 ramène à 0 ; cela ne veut pas dire que les entiers 4 et 5 sont égaux.

À toi d'essayer : Même reste ne signifie pas même nombre

Pourquoi $-8 \equiv 7 \pmod 5$? Donne leur reste commun, puis un module pour lequel ils ne sont pas congrus.
Pour démarrer. Soustrais les nombres, puis cherche leurs deux divisions euclidiennes.

Tu peux chercher, prendre un indice ou lire l'explication, à ton rythme.

Indices, p. 27 Explication, p. 30

3.4 Calculer avec les congruences

Théorème | Compatibilité

Si $a \equiv b \pmod n$ et $c \equiv d \pmod n$, alors

$$a + c \equiv b + d \pmod n, \qquad ac \equiv bd \pmod n.$$

On peut aussi soustraire, multiplier par un entier, et élever à une puissance entière positive ou nulle : $a^k \equiv b^k \pmod n$ pour $k \in \mathbb{N}$.

Démonstration | Les opérations permises

Les hypothèses signifient $a = b + nu$ et $c = d + nv$ pour des entiers u, v.
Pour les sommes, $(a + c) - (b + d) = (b + nu + d + nv) - (b + d) = n(u + v)$: leur différence est un multiple de n. Pour les différences, le même calcul donne $(a - c) - (b - d) = n(u - v)$.
Pour les produits, développons les quatre termes : $ac = (b+nu)(d+nv) = bd+bnv+dnu+n^2uv$. Donc $ac-bd = n(bv+du+nuv)$, encore un multiple de n car la parenthèse est entière. Cela autorise les remplacements dans une addition, une soustraction ou une multiplication.
Pour les puissances, au rang 0 les deux valeurs sont 1, donc congrues. Si $a^k \equiv b^k$, la propriété du produit, appliquée aussi à $a \equiv b$, donne $a^{k+1} = a^k a \equiv b^k b = b^{k+1}$. Par récurrence, la propriété vaut pour tout $k \geq 0$. Nous n'avons pas démontré de règle de division : elle nécessite d'autres conditions.

Exemple | Réduire avant de calculer

Les divisions $100 = 7 \times 14 + 2$ et $99 = 7 \times 14 + 1$ donnent $100 \equiv 2$ et $99 \equiv 1 \pmod 7$. Les puissances et les sommes respectent les congruences, donc $100^2 + 99^3 \equiv 2^2 + 1^3 = 4 + 1 = 5 \pmod 7$. Comme $0 \leq 5 < 7$, 5 est bien le reste euclidien demandé, pas seulement un représentant quelconque. Le calcul conserve le reste, sans affirmer que les grands nombres sont égaux à 2 et 1.

Attention | Ne pas simplifier sans condition

On ne peut pas toujours diviser une congruence par un facteur commun. Par exemple $2 \times 1 \equiv 2 \times 4 \pmod 6$, mais $1 \not\equiv 4 \pmod 6$. Ici, on peut seulement conclure $1 \equiv 4 \pmod 3$. L'inverse modulo n, étudié au chapitre suivant, précisera quand la simplification conserve le module.

Méthode | Un inverse déjà visible

Si tu as trouvé u tel que $au \equiv 1 \pmod{n}$, tu peux multiplier $ax \equiv b \pmod{n}$ par u, ce qui donne $x \equiv ub \pmod{n}$. Par exemple $3 \times 5 \equiv 1 \pmod{7}$; l'équation $3x \equiv 2 \pmod{7}$ donne $x \equiv 10 \equiv 3 \pmod{7}$.

À toi d'essayer : Réparer une simplification interdite

Résous $2x \equiv 2 \pmod{6}$ sans diviser abusivement en gardant le module 6.
Pour démarrer. Écris $2(x-1) = 6k$ avec k entier avant de simplifier.

Tu peux chercher, prendre un indice ou lire l'explication, à ton rythme.

Indices, p. 27 Explication, p. 30

3.5 Puissances et raisonnements par restes

Pour trouver $a^N \pmod{n}$, calcule quelques puissances réduites. Si $a^t \equiv 1 \pmod{n}$, écris $N = tq + r$: $a^N \equiv a^r$. Il faut avoir établi le cycle avant de l'utiliser.

Exemple | Dernier chiffre

Le dernier chiffre d'un entier est son reste modulo 10. Calculons les puissances successives : $3^1 \equiv 3$, $3^2 = 9$, $3^3 = 27 \equiv 7$, $3^4 = 81 \equiv 1$. Cette dernière égalité justifie le retour au début : multiplier à nouveau par 3 redonne 3.
Écrivons $2026 = 4 \times 506 + 2$. Alors $3^{2026} = (3^4)^{506} 3^2 \equiv 1^{506} \times 9 = 9 \pmod{10}$. Le dernier chiffre vaut donc 9. Nous réduisons l'exposant modulo 4, longueur du cycle démontré, et la valeur finale modulo 10 : ce sont deux rôles différents.

Méthode | Exclure une équation entière

Choisis un module pour lequel les carrés ou les puissances ont peu de restes. Liste les possibilités, puis montre que le membre demandé est impossible. L'absence de solution modulo n implique l'absence de solution entière ; la présence d'une solution modulaire ne prouve pas l'existence d'une solution entière.

Exemple | Carrés modulo 4

Tout entier est pair ou impair. Si $x = 2k$, alors $x^2 = 4k^2$, donc son reste modulo 4 est 0. Si $x = 2k+1$, alors $x^2 = 4k^2 + 4k + 1 = 4(k^2+k) + 1$, donc son reste est 1. Cela couvre tous les entiers, même négatifs.
Pour deux carrés, les sommes de restes possibles sont $0+0=0$, $0+1=1$, $1+0=1$, $1+1=2$. Aucune ne donne 3 modulo 4. Or $4m+3$ a précisément ce reste. Si une solution entière de $x^2+y^2 = 4m+3$ existait, l'égalité imposerait des restes égaux, ce qui est impossible. La contradiction exclut toute solution entière.

Une preuve à construire : Trois entiers consécutifs

Montre que $n(n+1)(n+2)$ est divisible par 3 pour tout entier relatif n.
Pour démarrer. Liste les trois restes possibles de n et repère le facteur de reste zéro.

Tu peux chercher, prendre un indice ou lire l'explication, à ton rythme.

Indices, p. 28 Explication, p. 31

À toi d'essayer : Une table de restes est une preuve finie

Quels restes peut prendre un carré modulo 3 ? Déduis que $x^2 + y^2 = 3m + 2$ impose x et y non divisibles par 3.
Pour démarrer. Construis la liste des carrés de 0, 1 et 2 modulo 3, puis celle de leurs sommes.

Tu peux chercher, prendre un indice ou lire l'explication, à ton rythme.

Indices, p. 28 Explication, p. 31

3.6 Démontrer les tests de divisibilité

Un entier naturel d'écriture décimale $a_m a_{m-1} \cdots a_0$ vaut $N = \sum_{k=0}^{m} a_k 10^k$, où chaque chiffre est entre 0 et 9.

Propriété | Tests issus de la base 10

Modulo 3 ou 9, $10 \equiv 1$ car $10 - 1 = 9$ est divisible par chacun de ces modules. En élevant à la puissance k, $10^k \equiv 1^k = 1$. Multiplier par a_k puis additionner donne $N \equiv a_0 + a_1 + \cdots + a_m$. Deux nombres congrus sont simultanément divisibles par le module, car avoir reste zéro pour l'un impose reste zéro pour l'autre. Cela prouve le test par somme des chiffres, dans les deux sens.
Modulo 11, $10 \equiv -1$ car $10 - (-1) = 11$. Donc $10^k \equiv (-1)^k$. Cette puissance vaut 1 si k est pair, -1 s'il est impair : $N \equiv a_0 - a_1 + a_2 - a_3 + \cdots$. Le premier signe positif correspond aux unités, car leur exposant est 0. Le même raisonnement sur le reste zéro donne le test par somme alternée.

Pour 2, 5 ou 10, écrivons $N = 10q + a_0$. Le module divise $10q$, donc $N \equiv a_0$: seul le chiffre des unités compte. Pour 4 ou 25, écrivons $N = 100q + (10a_1 + a_0)$. Comme 100 est multiple du module, le premier terme a reste zéro ; on teste donc l'entier formé par les deux derniers chiffres. Pour 8 ou 125, $1000 = 8 \times 125$ est multiple des deux modules : écrire $N = 1000q + r$, avec r formé des trois derniers chiffres, prouve de même $N \equiv r$.

Exemple | Tester 27 918

Pour 3 et 9, la somme des chiffres vaut $2+7+9+1+8 = 27$. Comme $27 = 3 \times 9 = 9 \times 3$, le nombre est divisible par les deux. Pour 11, on alterne les signes depuis les unités : $8 - 1 + 9 - 7 + 2 = 11$. Ce résultat étant multiple de 11, le nombre l'est également. Contrôle : $27918 = 11 \times 2538$.
Pour 4, seuls les deux derniers chiffres comptent : 18 a pour reste 2 modulo 4. Le nombre a donc ce même reste 2 et n'est pas divisible par 4. Chaque test correspond à un module différent ; réussir le test de 9 n'entraîne pas celui de 4.

À toi d'essayer : Retrouver un test par la base dix

Pourquoi les deux derniers chiffres suffisent-ils pour tester la divisibilité par 4 ?
Pour démarrer. Sépare la partie des centaines et le nombre formé par les deux derniers chiffres.

Tu peux chercher, prendre un indice ou lire l'explication, à ton rythme.

Indices, p. 28 Explication, p. 31

3.7 Algorithmes et précautions de programmation

Pour un diviseur positif, Python fournit quotient et reste via `//` et `%`. Il s'agit de la division avec quotient arrondi vers le bas, ce qui respecte la division euclidienne aussi pour un dividende négatif.

```python
def division(a, b):
    if b <= 0:
        raise ValueError("b doit etre positif")
    q, r = a // b, a % b
    return q, r

def puissance_mod(a, n, m):
    if n < 0 or m <= 0:
        raise ValueError("n >= 0 et m > 0 requis")
    resultat = 1 % m
    for _ in range(n):
        resultat = (resultat * a) % m
    return resultat
```

Avant la boucle. Aucun facteur a n'a encore été multiplié. La variable contient le reste de 1 modulo m, donc elle est congrue à $a^0 = 1$ et appartient à $\{0, \dots, m-1\}$. Cela reste vrai pour $m = 1$, où le seul reste est 0.

Pendant un tour. Supposons qu'après k tours, la variable soit congrue à a^k. La multiplier par a donne un nombre congru à a^{k+1}. L'opération `% m` remplace ce nombre par son reste : elle conserve la congruence et remet la valeur entre 0 et $m-1$. La propriété se transmet donc du rang k au rang $k+1$.

À la fin. La boucle a effectué exactement n tours, donc la variable est congrue à a^n et dans l'intervalle des restes. L'unicité de la division euclidienne prouve qu'elle contient le reste recherché. Si $n = 0$, aucun tour n'est exécuté et la valeur initiale convient déjà. Cette initialisation et cette transmission constituent une preuve par récurrence, appelée invariant de boucle. La fiche 6 réduira le nombre de multiplications pour les grands exposants.

À toi d'essayer : Prévoir le résultat du code

En Python avec un diviseur positif, prévois les valeurs de $-19\,\%\,6$ et $-19\,//\,6$ sans exécuter le code.
Pour démarrer. Encadre -19 entre deux multiples consécutifs de 6.

Tu peux chercher, prendre un indice ou lire l'explication, à ton rythme.

Indices, p. 28 Explication, p. 31

4 Boîte à outils — chercher le bon module

4.1 Une équation impossible modulo 3

Exemple | Résoudre une question d'existence

Supposons $x^2 = 3y + 2$ avec x, y entiers. Le reste de x modulo 3 est l'un des trois nombres 0,1,2. Les carrés correspondants sont $0^2 = 0$, $1^2 = 1$, $2^2 = 4 \equiv 1$. Donc x^2 ne peut avoir que les restes 0 ou 1.
Le membre droit est $3y+2$, de reste 2. Une égalité entre entiers imposerait le même reste aux deux membres ; ici c'est impossible. Il n'existe donc aucun couple entier solution. Le choix du module 3 vient du terme $3y$, qui disparaît modulo 3 et laisse une seule valeur à comparer.

4.2 Un chiffre inconnu dans une écriture décimale

La somme des chiffres de $4a32$ vaut $4 + a + 3 + 2 = a + 9$. Puisque a est un chiffre, $0 \leq a \leq 9$, donc $9 \leq a+9 \leq 18$. Les seuls multiples de 9 dans cet intervalle sont 9 et 18. Résoudre $a+9 = 9$ donne $a = 0$; résoudre $a+9 = 18$ donne $a = 9$. On obtient donc exactement 4032 et 4932. Les contrôles $9 \times 448 = 4032$ et $9 \times 548 = 4932$ confirment les deux solutions.

Si l'on ajoute la divisibilité par 11, la somme alternée depuis les unités vaut $2 - 3 + a - 4 = a - 5$. Parmi les chiffres autorisés, seul a=5 satisferait ce second test. Aucun chiffre ne satisfait donc simultanément les deux tests. Le domaine des chiffres, de 0 à 9, est une donnée essentielle du problème.

4.3 Un cycle n'est pas toujours immédiatement inversible

Exemple | Puissances de 2 modulo 8

Les premières puissances donnent $2^0 = 1$, $2^1 = 2$, $2^2 = 4$, puis $2^3 = 8 \equiv 0 \pmod 8$. Pour tout $n \geq 3$, $2^n = 2^3 \times 2^{n-3} = 8 \times 2^{n-3}$ est un multiple de 8, donc son reste reste 0.
La suite des restes est $1, 2, 4, 0, 0, \ldots$: elle ne revient pas à 1. On ne peut pas inventer une période de longueur 3 à partir des trois premières valeurs. La factorisation prouve exactement à partir de quel rang le reste est nul.

4.4 Passer d'une congruence à tous les entiers

L'écriture $x \equiv 4 \pmod 7$ ne signifie pas seulement x=4. Elle équivaut à $x = 4 + 7k$ pour un entier k, positif, nul ou négatif. Si une contrainte supplémentaire impose $0 \leq x \leq 30$, alors $0 \leq 4 + 7k \leq 30$, donc k=0,1,2,3 ; les valeurs sont 4,11,18,25. Les contraintes d'intervalle viennent après la résolution modulaire.

À toi d'essayer : Retrouver un chiffre

Quel chiffre a rend le nombre $7a5$ divisible par 9 ?
Pour démarrer. Utilise le test de 9 et rappelle qu'un chiffre est compris entre 0 et 9.

Tu peux chercher, prendre un indice ou lire l'explication, à ton rythme.

Indices, p. 29 Explication, p. 31

À toi d'essayer : Réduire deux bases

Calcule le reste de $2^{100} + 3^{100}$ modulo 8.
Pour démarrer. Pour 2^{100}, extrais un facteur 8 ; pour 3^{100}, groupe les facteurs par deux.

Tu peux chercher, prendre un indice ou lire l'explication, à ton rythme.

Indices, p. 29 Explication, p. 32

5 Exercices progressifs

Les exercices 1 à 5 consolident les bases, 6 à 10 relient les notions et 11 à 15 demandent davantage d'initiative. Cherche d'abord, puis utilise un indice si tu en as besoin.

Exercice 1 — Diviseurs signés ⭐☆☆

Liste les diviseurs entiers de 18. Justifie $-6 \mid 18$ et décide si $0 \mid 18$.

Exercice 2 — Division positive ⭐☆☆

Donne la division euclidienne de 173 par 12.

Exercice 3 — Division négative ⭐☆☆

Divise euclidiennement -59 par 7.

Exercice 4 — Lire une congruence ⭐☆☆

Décide si $38 \equiv 3 \pmod 7$, $-17 \equiv 3 \pmod 5$ et $21 \equiv 1 \pmod 6$.

Exercice 5 — Réduction préalable ⭐☆☆

Calcule le reste de $52 \times 79 + 100$ modulo 9.

Exercice 6 — Un facteur constant ⭐⭐☆

Montre que tout diviseur commun à $5n + 2$ et $3n + 1$ divise 1.

Exercice 7 — Puissance modulo 7 ⭐⭐☆

Détermine le reste de 2^{100} modulo 7.

Exercice 8 — Dernier chiffre ⭐⭐☆

Détermine le dernier chiffre de 7^{2026}.

Exercice 9 — Tester un nombre ⭐⭐☆

Le nombre 123 456 est-il divisible par 3, 9, 4 et 11 ?

Exercice 10 — Inverse visible ⭐⭐☆

Résous $5x \equiv 3 \pmod 7$.

Exercice 11 — Une simplification fausse ⭐⭐⭐

Trouve toutes les solutions modulo 6 de $2x \equiv 2 \pmod 6$ et explique pourquoi $x \equiv 1 \pmod 6$ est incomplet.

Exercice 12 — Une impossibilité entière ⭐⭐⭐

Montre qu'aucun entier n ne vérifie $n^2 = 2027$.

Exercice 13 — Divisibilité universelle ⭐⭐⭐

Démontre que $n^3 - n$ est divisible par 6 pour tout $n \in \mathbb{Z}$.

Garder le reste pour comprendre les entiers.

Exercice 14 — Un test pour 7 ⭐⭐⭐

Écris $N = 10a + b$, où b est le chiffre des unités. Montre que N est divisible par 7 si et seulement si $a - 2b$ l'est. Applique à 203.

Exercice 15 — Lire un algorithme ⭐⭐⭐

Que renvoie `puissance_mod(3, 5, 7)` ? Justifie la fonction et explique le cas n=0.

6 🚀 Problème — Pour aller plus loin

Ce prolongement est accessible à partir du cours : les résultats supplémentaires sont guidés, et leur mémorisation n'est pas un préalable. Tu peux répartir la recherche sur plusieurs séances.

Construire et casser un chiffrement affine

On code les lettres A à Z par les entiers 0 à 25. Une lettre de code x est transformée en la lettre de code y, reste de $5x + 8$ modulo 26. Espaces et accents sont retirés. Ce modèle sert à apprendre ; il ne prétend pas protéger un message réel. Durée indicative : 60 à 90 minutes.

Partie I — Chiffrer

1. Chiffre le mot MATHS en détaillant les cinq restes.
2. Montre que $5 \times 21 \equiv 1 \pmod{26}$.
3. Démontre que deux codes donnant la même image sont congrus modulo 26 ; explique pourquoi deux lettres différentes ne se confondent pas.

Partie II — Déchiffrer

1. À partir de $y \equiv 5x + 8$, exprime x modulo 26 en fonction de y.
2. Déchiffre IZ et vérifie en rechiffrant.
3. Que se passe-t-il si l'on remplace le coefficient 5 par 2 ? Donne deux lettres différentes ayant la même image.

Partie III — Retrouver une clé

On sait qu'un chiffrement $y \equiv ax + b \pmod{26}$ envoie A sur I et B sur N.

1. Retrouve b puis a modulo 26.
2. Rédige deux fonctions Python de chiffrement et déchiffrement d'un code entier.
3. Explique pourquoi la connaissance de deux lettres consécutives et de leurs images suffit ici à retrouver la clé.

Pistes

M vaut 12, A vaut 0, T vaut 19, H vaut 7 et S vaut 18. Pour déchiffrer, soustrais 8 puis multiplie par 21. Pour la clé inconnue, A et B ont pour codes 0 et 1.

7 Indices des exercices

Exercice 1

Commence par les diviseurs positifs.

Ajoute leurs opposés.

Exercice 2

Cherche le plus grand multiple inférieur au dividende.

Vérifie la borne du reste.

Exercice 3

Le quotient est l'entier inférieur à -59/7.

Si le reste est négatif, diminue le quotient de 1.

Exercice 4

Soustrais les deux nombres.

Teste la divisibilité par le module indiqué.

Exercice 5

Réduis chaque entier avant de multiplier.

Réduis aussi le résultat final.

Exercice 6

Cherche des coefficients qui éliminent n.

Utilise 3 et -5.

Exercice 7

Cherche une puissance égale à 1 modulo 7.

Divise l'exposant par la longueur du cycle.

Exercice 8

Travaille modulo 10.

Justifie la période avec la puissance quatrième.

Exercice 9

Applique les tests démontrés.

Pour 11, garde l'alternance des signes.

Exercice 10

Cherche un petit multiple de 5 congru à 1.

Vérifie la classe de solutions.

Exercice 11

Reviens à une divisibilité.

Le module doit aussi être divisé ici.

Exercice 12

Étudie les carrés modulo 4.

Distingue un entier pair et un entier impair.

Exercice 13

Factorise avant de calculer des restes.

Repère un facteur 2 et un facteur 3 dans le produit.

Exercice 14

Compare N à dix fois la quantité proposée.

Justifie la simplification grâce à un inverse de 3 modulo 7.

Exercice 15

Construis une table des valeurs après chaque tour.

Distingue initialisation, conservation et arrêt.

8 Corrigés détaillés

Corrigé 1

Démonstration / Solution expliquée

Cherchons les paires de facteurs positifs de 18 : 1×18, 2×9 et 3×6. Elles fournissent les diviseurs positifs $1, 2, 3, 6, 9, 18$. Leurs opposés divisent aussi 18, en changeant également le signe du quotient. La liste entière est donc $\pm 1, \pm 2, \pm 3, \pm 6, \pm 9, \pm 18$.
En particulier, $18 = (-6)(-3)$ exhibe un quotient entier et prouve $-6 \mid 18$. En revanche, $0 \mid 18$ demanderait un entier k tel que $18 = 0k$. Le membre droit vaut toujours zéro : c'est impossible.

Corrigé 2

Démonstration / Solution expliquée

Les multiples voisins sont $12 \times 14 = 168$ et $12 \times 15 = 180$. On a $168 \leq 173 < 180$, donc le quotient est 14. Le reste vaut $173 - 168 = 5$. Ainsi $173 = 12 \times 14 + 5$.
Deux contrôles sont nécessaires : la somme vaut bien 173, et $0 \leq 5 < 12$. Ils prouvent que $(q, r) = (14, 5)$ est la division euclidienne. Un quotient 13 donnerait un reste 17, qui satisferait l'égalité mais pas la borne du reste.

Corrigé 3

Démonstration / Solution expliquée

Les multiples de 7 qui encadrent -59 sont $-63 = 7(-9)$ et $-56 = 7(-8)$. Le multiple inférieur est -63, donc $q = -9$. Le reste est $r = -59 - (-63) = 4$.
La réponse est $-59 = 7(-9) + 4$, avec $0 \leq 4 < 7$. Si l'on prenait $q = -8$, le reste serait $-59 + 56 = -3$, interdit. Il faut arrondir le quotient vers le bas, pas vers zéro.

Corrigé 4

Démonstration / Solution expliquée

Une congruence se teste par la divisibilité de la différence. Pour la première, $38 - 3 = 35 = 7 \times 5$: elle est vraie. Pour la deuxième, $-17 - 3 = -20 = 5(-4)$: un quotient négatif est autorisé, donc elle est vraie aussi.
Pour la troisième, $21 - 1 = 20 = 6 \times 3 + 2$, qui n'est pas divisible par 6. Elle est donc fausse. On peut aussi comparer les restes : 21 a pour reste 3 modulo 6, tandis que 1 a pour reste 1.

Corrigé 5

Démonstration / Solution expliquée

Les divisions donnent $52 = 9 \times 5 + 7$, $79 = 9 \times 8 + 7$ et $100 = 9 \times 11 + 1$. Remplaçons chaque nombre par son reste, ce qui est permis dans le produit et la somme : $52 \times 79 + 100 \equiv 7 \times 7 + 1 = 50 \pmod 9$.
Le nombre 50 n'est pas encore un reste autorisé puisqu'il dépasse 8. Sa division $50 = 9 \times 5 + 5$ donne le reste final 5. Pour contrôle direct, l'entier initial vaut 4208 et $4208 = 9 \times 467 + 5$.

Corrigé 6

Démonstration | Solution expliquée

Soit d un diviseur des deux expressions. Par la règle des combinaisons entières, il divise $3(5n+2) - 5(3n+1)$. Les coefficients 3 et -5 ont été choisis pour annuler $15n$.
Développons : $15n + 6 - 15n - 5 = 1$. Donc $d \mid 1$. Cela impose $d = 1$ ou $d = -1$. Réciproquement, ces deux entiers divisent toute expression entière ; ce sont donc exactement les diviseurs communs, quel que soit n.

Corrigé 7

Démonstration | Solution expliquée

Nous cherchons une puissance de 2 qui revienne au reste 1 modulo 7. Les premières sont $2, 4, 8$, et $8 = 7 + 1$, donc $2^3 \equiv 1 \pmod 7$.
Divisons l'exposant par 3 : $100 = 3 \times 33 + 1$. La règle des puissances donne $2^{100} = (2^3)^{33}2$. Modulo 7, cela vaut $1^{33} \times 2 = 2$. Puisque 2 est compris entre 0 et 6, c'est le reste euclidien. La base est calculée modulo 7, l'exposant est partagé en groupes de 3.

Corrigé 8

Démonstration | Solution expliquée

Le dernier chiffre est un reste modulo 10. On calcule $7^1 \equiv 7$, $7^2 = 49 \equiv 9$, $7^3 \equiv 9 \times 7 = 63 \equiv 3$, $7^4 \equiv 3 \times 7 = 21 \equiv 1$.
Comme $2026 = 4 \times 506 + 2$, $7^{2026} = (7^4)^{506}7^2 \equiv 1^{506} \times 9 = 9 \pmod{10}$. Le dernier chiffre est 9. Le retour à 1 justifie la répétition ; une simple liste de premiers termes, sans cette justification, ne prouverait pas la suite du calcul.

Corrigé 9

Démonstration | Solution expliquée

La somme des chiffres est $1 + 2 + 3 + 4 + 5 + 6 = 21$. Son reste modulo 3 est 0, donc 123456 est divisible par 3. Son reste modulo 9 est 3, donc il n'est pas divisible par 9.
Pour 4, le nombre formé par les deux derniers chiffres est 56, et $56 = 4 \times 14$: la divisibilité est vraie.
Pour 11, la somme alternée depuis les unités est $6 - 5 + 4 - 3 + 2 - 1 = 3$. Ce n'est pas un multiple de 11, donc la divisibilité est fausse. Chaque conclusion applique le test au bon module ; la seule taille de la somme des chiffres ne suffit pas.

Corrigé 10

Démonstration | Solution expliquée

On ne divise pas directement par 5 dans une congruence. Cherchons son inverse : $5 \times 3 = 15 = 2 \times 7 + 1$, donc multiplier par 3 annule le facteur 5 modulo 7. Ainsi $5x \equiv 3$ entraîne $15x \equiv 9$, soit $x \equiv 2 \pmod 7$.

Cela signifie $x = 2+7k$, $k \in \mathbb{Z}$. Vérifions la réciproque pour toute la famille : $5x-3 = 5(2+7k)-3 = 7+35k = 7(1+5k)$, multiple de 7. Toutes ces valeurs conviennent, et l'étape par l'inverse prouve qu'il n'y en a pas d'autres.

Corrigé 11

Démonstration / Solution expliquée

Revenons à la définition : $2x \equiv 2 \pmod 6$ signifie $2x-2 = 6k$ pour un entier k. Dans cette *égalité*, on peut diviser les deux membres par 2 : $x-1 = 3k$, donc $x = 1+3k$.
Si $k = 2m$ est pair, $x = 1+6m$ a pour reste 1 modulo 6. Si $k = 2m+1$ est impair, $x = 4+6m$ a pour reste 4. Les deux restes 1 et 4 conviennent : $2 \times 1 = 2$ et $2 \times 4 = 8 \equiv 2$. Écrire seulement $x \equiv 1 \pmod 6$ supprimerait donc les valeurs de reste 4.

Corrigé 12

Démonstration / Solution expliquée

La division $2027 = 4 \times 506 + 3$ donne le reste 3 modulo 4. Mais un entier pair $n = 2k$ a pour carré $4k^2$, de reste 0. Un entier impair $n = 2k+1$ a pour carré $4(k^2+k)+1$, de reste 1.
Tous les entiers sont pairs ou impairs ; aucun carré entier n'a donc le reste 3. Si $n^2 = 2027$ était vrai, leurs restes seraient égaux, contradiction. L'équation n'a aucune solution dans $\mathbb{Z}$, sans avoir besoin d'une approximation décimale de la racine.

Corrigé 13

Démonstration / Solution expliquée

Factorisons : $n^3 - n = n(n^2-1) = (n-1)n(n+1)$. Parmi ces trois entiers consécutifs, l'un est multiple de 3 ; parmi deux consécutifs, l'un est pair, donc le produit possède aussi un facteur 2.
Il faut justifier que ces facteurs donnent bien un facteur 6. Si le multiple de 3 est pair, écrivons-le $3k$; sa parité impose k pair, donc il vaut 6ℓ. Sinon il est impair, et le facteur pair se trouve parmi les deux autres : en écrivant ces facteurs $3k$ et 2ℓ, leur produit contient $6k\ell$. Dans les deux cas, le produit total est un multiple de 6. L'argument vaut aussi lorsque l'un des facteurs est zéro.

Corrigé 14

Démonstration / Solution expliquée

Posons $T = a-2b$. Calculons $N - 10T = (10a+b) - 10(a-2b) = 10a+b-10a+20b = 21b$, multiple de 7. Donc $N \equiv 10T \equiv 3T \pmod 7$.
Si $T \equiv 0$, alors $N \equiv 0$. Inversement, si $N \equiv 0$, $3T \equiv 0$; multiplier par 5 est permis et donne $15T \equiv 0$, soit $T \equiv 0$ puisque $15 \equiv 1 \pmod 7$. Les deux sens prouvent l'équivalence.
Pour 203, $a = 20, b = 3$, donc $T = 20-6 = 14$, multiple de 7. Ainsi 203 est divisible par 7 ; vérification : $203 = 7 \times 29$.

Corrigé 15

Démonstration / Solution expliquée

La variable commence à 1. Les cinq tours calculent successivement les restes de $1 \times 3 = 3$, $3 \times 3 = 9 \equiv 2$, $2 \times 3 = 6$, $6 \times 3 = 18 \equiv 4$, $4 \times 3 = 12 \equiv 5$ modulo 7. La fonction renvoie donc 5.
Pour justifier toutes les entrées, au départ le résultat est le reste de $a^0 = 1$. Supposons qu'après k tours il soit congru à a^k. Le tour suivant multiplie par a, donc donne un nombre congru à a^{k+1} ; la réduction modulo m le ramène entre 0 et $m - 1$. Après n tours, c'est donc le reste de a^n. Si $n = 0$, aucun tour n'a lieu et le résultat est $1 \bmod m$. Pour $m = 1$, tous les restes valent 0, y compris celui de 1.

9 Corrigé du problème

Partie I — Calculer les cinq images

1. Les codes de M,A,T,H,S sont 12,0,19,7,18. La transformation ajoute 8 après multiplication par 5, puis garde le reste entre 0 et 25 :

$$\begin{aligned} 5\times 12+8 &= 68 = 2\times 26+16 && \text{donne Q},\\ 5\times 0+8 &= 8 = 0\times 26+8 && \text{donne I},\\ 5\times 19+8 &= 103 = 3\times 26+25 && \text{donne Z},\\ 5\times 7+8 &= 43 = 1\times 26+17 && \text{donne R},\\ 5\times 18+8 &= 98 = 3\times 26+20 && \text{donne U}. \end{aligned}$$

Le mot chiffré est QIZRU. Chaque reste, et non le quotient, détermine la lettre.

2. $5\times 21 = 105 = 4\times 26+1$, donc $5\times 21\equiv 1 \pmod{26}$. Le nombre 21 est un inverse de 5 modulo 26.

3. Supposons deux images égales. Alors $5x+8\equiv 5x'+8$. Soustraire 8 puis $5x'$ donne $5(x-x')\equiv 0$. Multiplier par 21 donne $x-x'\equiv 0$ puisque $105\equiv 1$. Les codes x, x' sont entre 0 et 25, donc leur différence est entre -25 et 25. Le seul multiple de 26 dans cet intervalle est zéro : $x=x'$. Deux lettres distinctes ne peuvent donc pas se confondre.

Partie II — Remonter chaque opération

1. À partir de $y\equiv 5x+8$, soustrayons 8 : $y-8\equiv 5x$. Multiplions ensuite par 21 : $21(y-8)\equiv 105x\equiv x$. Le déchiffrement consiste donc à prendre le reste de $21(y-8)$ modulo 26. L'ordre compte : on retire d'abord le décalage, puis on annule la multiplication.

2. Pour I, $y=8$, donc $21(y-8)=0$ et le code initial est 0, soit A. Pour Z, $y=25$, donc $21(25-8)=21\times 17=357=13\times 26+19$. Le code 19 est T. Ainsi IZ devient AT. Rechiffrons : A donne $5\times 0+8=8$, donc I ; T donne 103 de reste 25, donc Z. La vérification retrouve le message chiffré.

3. Avec le coefficient 2, le code 0 donne $2\times 0+8=8$; le code 13 donne $2\times 13+8=34=26+8$. Les lettres A et N ont donc toutes deux pour image I. Une image ne permet plus de choisir un antécédent unique. Cette collision explique concrètement pourquoi on ne peut pas simplement diviser par 2 modulo 26.

Partie III — Retrouver puis programmer la clé

1. A a pour code 0 et I pour code 8. Donc $a \times 0 + b \equiv 8$, soit $b \equiv 8$. B a pour code 1 et N pour code 13 ; $a + b \equiv 13$. Soustraire la première congruence donne $a \equiv 13 - 8 = 5$. La clé est donc $a = 5, b = 8$ modulo 26.

2. Les fonctions prennent un code entier et renvoient un code entre 0 et 25 :

```
def chiffre(x):
    return (5*x + 8) % 26

def dechiffre(y):
    return (21*(y - 8)) % 26
```

L'opérateur `% 26` impose le reste autorisé, même si $y-8$ est négatif. Les parenthèses de la seconde fonction assurent que la soustraction a lieu avant la multiplication. Pour tout code x, la composition donne modulo 26 $21((5x + 8) - 8) = 105x \equiv x$. Comme le résultat et x sont tous deux entre 0 et 25, ils sont égaux.

3. Pour deux codes consécutifs x et $x + 1$, les images sont congrues à $ax + b$ et $a(x + 1) + b = ax + a + b$. Leur différence est donc congrue à a. Une fois a connu, $b \equiv y - ax$ le détermine aussi. Pour des codes non consécutifs, on obtiendrait un multiple de a ; l'annuler demanderait un inverse qui pourrait ne pas exister. L'argument repose donc bien sur la différence égale à 1.

10 Faire le point par une variante autonome

Essaie cette variante sans relire le corrigé précédent. Explique le choix de ta méthode, puis utilise les contrôles pour décider quelle notion retravailler.

À toi d'essayer : Une puissance et une conclusion entière

Trouve le reste de 7^{2026} modulo 5, puis décide si $7^{2026}+1$ est divisible par 5.
Pour démarrer. Réduis la base modulo 5, puis démontre une puissance de retour à 1.

Tu peux chercher, prendre un indice ou lire l'explication, à ton rythme.

Indices, p. 29 Explication, p. 32

11 Fiche-mémoire

— $a \mid b$ signifie $b = ak$ pour un entier k.
— Division euclidienne : $a = bq + r$ avec $b > 0$ et $0 \leq r < b$.
— $a \equiv b \pmod{n}$ signifie $n \mid (a - b)$, ou mêmes restes.
— Addition, soustraction, produit et puissances positives conservent une congruence.
— Une division exige une justification ; un inverse modulaire permet de simplifier.
— Un test de divisibilité découle des puissances de 10 modulo le diviseur.

Autocontrôle. Mes quotients sont-ils entiers ? Le reste est-il dans le bon intervalle ? Ai-je conservé le module ? Ai-je prouvé la période des puissances ? Ai-je vérifié la réciproque d'une équivalence ?

12 Indices des pauses et des preuves

Chercher avec un indice fait partie du travail. Tu peux revenir à l'énoncé avec le lien sous chaque aide.

Transformer le symbole en égalité

Indice 1 — Une piste.

Écris $a = du$ et $b = dv$ avec u,v entiers.

Indice 2 — Un pas de plus.

Factorise d dans la combinaison.

Revenir à la recherche, p. 5

Corriger un reste

Indice 1 — Une piste.

Le reste doit être positif ou nul.

Indice 2 — Un pas de plus.

Remplace -4 par -5 et compense.

Revenir à la recherche, p. 7

Même reste ne signifie pas même nombre

Indice 1 — Une piste.

La différence vaut moins quinze.

Indice 2 — Un pas de plus.

Écris $-8 = 5(-2) + 2$ et $7 = 5 + 2$.

Revenir à la recherche, p. 8

Réparer une simplification interdite

Indice 1 — Une piste.

Écris la divisibilité de 2x moins 2 par 6.

Indice 2 — Un pas de plus.

$2(x-1) = 6k$ équivaut à $x - 1 = 3k$.

Revenir à la recherche, p. 9

Trois entiers consécutifs

Indice 1 — Une piste.

Examine le reste de n modulo 3.

Indice 2 — Un pas de plus.

Parmi trois entiers consécutifs, l'un a un reste nul.

Revenir à la recherche, p. 10

Une table de restes est une preuve finie

Indice 1 — Une piste.

Teste les trois restes 0, 1 et 2.

Indice 2 — Un pas de plus.

Pour obtenir 2, quelle somme de deux restes parmi 0 et 1 convient ?

Revenir à la recherche, p. 10

Retrouver un test par la base dix

Indice 1 — Une piste.

Écris le nombre sous la forme $100q + r$, avec $0 \leq r < 100$.

Indice 2 — Un pas de plus.

100 est un multiple de 4.

Revenir à la recherche, p. 11

Prévoir le résultat du code

Indice 1 — Une piste.

Cherche un reste entre 0 et 5.

Indice 2 — Un pas de plus.

Le multiple de 6 immédiatement inférieur à -19 est -24.

Revenir à la recherche, p. 12

Retrouver un chiffre

Indice 1 — Une piste.

Calcule la somme des chiffres.

Indice 2 — Un pas de plus.

a+12 doit être un multiple de 9 compris entre 12 et 21.

Revenir à la recherche, p. 13

Réduire deux bases

Indice 1 — Une piste.

Traite séparément les deux puissances.

Indice 2 — Un pas de plus.

La première est divisible par 8 ; pour la seconde, utilise $3^2 \equiv 1$.

Revenir à la recherche, p. 13

Une puissance et une conclusion entière

Indice 1 — Une piste.

La base est congrue à 2.

Indice 2 — Un pas de plus.

$2^4 \equiv 1 \pmod 5$ et $2026 = 4 \times 506 + 2$.

Revenir à la recherche, p. 25

13 Explications des pauses et des preuves

Lis une étape, puis essaie de poursuivre avant de lire la suivante. Les calculs ci-dessous complètent le cours.

Transformer le symbole en égalité

Puisque $d \mid a$, il existe $u \in \mathbb{Z}$ tel que $a = du$; de même $b = dv$ avec $v \in \mathbb{Z}$. Alors $5a - 2b = 5du - 2dv = d(5u - 2v)$. La parenthèse est entière, ce qui prouve la divisibilité par définition. Avec des coefficients réels arbitraires, ce quotient ne serait plus garanti entier : 2 divise 2, mais multiplier 2 par $1/2$ donne 1, que 2 ne divise pas. La nature entière des coefficients est donc une hypothèse utilisée dans la preuve.

Revenir à la recherche, p. 5

Corriger un reste

L'égalité initiale est vraie mais son reste -1 est négatif. Remplacer -4 par -5 retire 4 au produit, donc il faut ajouter 4 au reste : $-1 + 4 = 3$. Ainsi $-17 = 4(-5) + 3$. Le calcul $-20 + 3 = -17$ vérifie l'égalité et $0 \leq 3 < 4$ vérifie la borne. Pour -18, le même quotient donne $r = -18 - (-20) = 2$, donc $-18 = 4(-5) + 2$, avec un reste encore autorisé.

Revenir à la recherche, p. 7

Même reste ne signifie pas même nombre

La différence est $-8 - 7 = -15 = 5(-3)$, donc les deux nombres sont congrus modulo 5. Les divisions confirment $-8 = 5(-2) + 2$ et $7 = 5 \times 1 + 2$: même reste 2. Modulo 2, en revanche, $-8 = 2(-4)$ a reste 0 et $7 = 2 \times 3 + 1$ a reste 1. Ils ne sont donc pas congrus modulo 2. Une congruence indique une égalité de restes relativement à un module précis, pas une égalité des nombres.

Revenir à la recherche, p. 8

Réparer une simplification interdite

La définition donne $6 \mid (2x - 2)$, soit $2(x - 1) = 6k$ pour un entier k. Diviser cette égalité par 2 donne $x - 1 = 3k$, donc les solutions sont $x = 1 + 3k$. Pour k pair, elles ont reste 1 modulo 6 ; pour k impair, reste 4. Les valeurs 1 et 4 vérifient bien l'équation initiale puisque $2 \times 1 = 2$ et $2 \times 4 = 8 = 6 + 2$. Le module devient 3 après la simplification ; conserver 6 ferait perdre une classe.

Revenir à la recherche, p. 9

Trois entiers consécutifs

Si $n = 3k$, le premier facteur est divisible par 3. Si $n = 3k+1$, alors $n+2 = 3k+3 = 3(k+1)$ l'est. Si $n = 3k+2$, alors $n+1 = 3k+3$ l'est. Dans chaque cas, le produit contient un facteur 3ℓ et peut s'écrire 3 fois un entier. Ces trois restes couvrent tout $n \in \mathbb{Z}$, y compris négatif. Pour la variante, parmi n et $n+1$, l'un est pair : si n est impair, son successeur est pair. Le produit contient donc aussi un facteur 2.

Revenir à la recherche, p. 10

Une table de restes est une preuve finie

Les restes possibles de x sont 0,1,2 ; leurs carrés donnent 0,1,4, soit 0,1,1 modulo 3. Un carré n'a donc que les restes 0 ou 1. Pour que $x^2 + y^2$ ait le reste 2, les quatre sommes possibles sont $0+0=0$, $0+1=1$, $1+0=1$, $1+1=2$: seule la dernière convient. Chaque carré doit donc avoir reste 1. Cela exclut que x ou y soit divisible par 3, car son carré aurait alors reste 0. La condition est nécessaire pour une solution, mais ne suffit pas à résoudre l'équation entière pour un m donné.

Revenir à la recherche, p. 10

Retrouver un test par la base dix

Tout entier naturel s'écrit $N = 100q + r$ avec $0 \leq r < 100$. Le nombre r correspond aux deux derniers chiffres, y compris un zéro initial éventuel. Comme $100 = 4 \times 25$, $N - r = 4(25q)$ est divisible par 4. Donc N et r ont le même reste modulo 4 : l'un est divisible par 4 si et seulement si l'autre l'est. Pour 3128, $r = 28 = 4 \times 7$; donc 3128 est divisible par 4. En effet $3128 = 4 \times 782$.

Revenir à la recherche, p. 11

Prévoir le résultat du code

Les multiples voisins sont $6(-4) = -24$ et $6(-3) = -18$. Le multiple inférieur est -24, et $-19-(-24) = 5$. Donc $-19 = 6(-4)+5$, avec $0 \leq 5 < 6$. Python renvoie ainsi 5 pour `-19 % 6` et -4 pour `-19 // 6`. Un quotient -3 donnerait un reste -1 ; ce serait une troncature vers zéro, qui ne respecte pas le reste positif utilisé par Python avec un diviseur positif.

Revenir à la recherche, p. 12

Retrouver un chiffre

La somme des chiffres de $7a5$ vaut $7 + a + 5 = a + 12$. Comme $0 \leq a \leq 9$, cette somme est entre 12 et 21. Les multiples de 9 voisins sont 9,18,27 ; seul 18 est dans cet intervalle. Il faut donc $a + 12 = 18$, soit $a = 6$. Cette valeur est bien un chiffre. Le nombre est 765, et $765 = 9 \times 85$ confirme la divisibilité. L'intervalle a permis de prouver qu'aucun autre chiffre ne convient.

Revenir à la recherche, p. 13

Réduire deux bases

Comme $100 \geq 3$, $2^{100} = 2^3 \times 2^{97} = 8 \times 2^{97}$, donc son reste modulo 8 est 0. Pour l'autre terme, $3^2 = 9 \equiv 1 \pmod 8$ et $100 = 2 \times 50$, donc $3^{100} = (3^2)^{50} \equiv 1^{50} = 1$. La somme a donc reste $0 + 1 = 1$. Le premier terme devient définitivement nul modulo 8 ; le second utilise un retour périodique au reste 1. On ne traite pas les deux bases avec un cycle supposé commun.

Revenir à la recherche, p. 13

Une puissance et une conclusion entière

Comme $7 = 5 + 2$, $7^{2026} \equiv 2^{2026} \pmod 5$. Or $2^4 = 16 \equiv 1 \pmod 5$ et $2026 = 4 \times 506 + 2$. Donc $2^{2026} = (2^4)^{506} 2^2 \equiv 1^{506} \times 4 = 4$. C'est le reste, car $0 \leq 4 < 5$. Ajouter 1 donne $7^{2026} + 1 \equiv 0 \pmod 5$, donc l'entier est divisible par 5. L'exposant a été partagé modulo 4 grâce au cycle, et non modulo 5 : la justification vient de $2^4 \equiv 1$.

Revenir à la recherche, p. 25