

PGCD, Bézout et Gauss — Terminale maths expertes

20 exercices corrigés · mathlvl.fr

Énoncés et corrigés détaillés

Présentation

L'algorithme d'Euclide fait bien plus que calculer un PGCD : en le remontant, il exprime ce PGCD comme combinaison $au + bv$ des deux nombres de départ. De cette identité de Bézout découle tout le reste — le critère de primalité entre deux entiers, le théorème de Gauss, l'inverse d'un nombre modulo n , et la résolution complète des équations $ax + by = c$ en nombres entiers. Ces 20 exercices corrigés couvrent l'ensemble du chapitre en maths expertes : PGCD par les diviseurs, par la décomposition et par l'algorithme d'Euclide, relation entre PGCD et PPCM, nombres premiers entre eux, coefficients de Bézout par remontée, théorème de Gauss et ses applications, équations diophantiennes avec solutions générales puis solutions positives, PGCD dépendant d'un paramètre, systèmes de congruences et chiffrement affine. Chaque correction est rédigée pas à pas, avec la vérification du résultat.

Version en ligne, avec les corrections dépliantes :

mathlvl.fr/exercices-corriges/terminale-maths-expertes/pgcd-bezout-gauss

Exercice 1 - PGCD par les diviseurs et par la décomposition

Le PGCD de deux entiers non nuls est le plus grand de leurs diviseurs communs. Deux méthodes élémentaires permettent de l'obtenir : lister les diviseurs, ou décomposer en facteurs premiers.

1. Déterminer les diviseurs positifs communs de 84 et 60, puis leur PGCD.
2. Retrouver ce PGCD par décomposition en facteurs premiers.
3. En déduire le PPCM de 84 et 60.

Exercice 2 - Algorithme d'Euclide

Lister les diviseurs devient impraticable dès que les nombres grandissent. L'algorithme d'Euclide repose sur une propriété simple : $\text{PGCD}(a; b) = \text{PGCD}(b; r)$ où r est le reste de a par b . On divise, on remplace, on recommence — le dernier reste non nul est le PGCD.

1. Calculer $\text{PGCD}(1071; 462)$ par l'algorithme d'Euclide.
2. Calculer $\text{PGCD}(255; 108)$.
3. Justifier la propriété $\text{PGCD}(a; b) = \text{PGCD}(b; r)$.

Exercice 3 - PGCD, PPCM et leur relation

Le PPCM de deux entiers est le plus petit de leurs multiples communs strictement positifs. Il est lié au PGCD par une relation qui permet de calculer l'un dès qu'on connaît l'autre.

1. Calculer $\text{PGCD}(1071; 462)$ puis $\text{PPCM}(1071; 462)$.
2. Deux feux clignotent, l'un toutes les 12 secondes, l'autre toutes les 18 secondes. Ils viennent de clignoter ensemble : dans combien de temps le feront-ils à nouveau ?

3. Deux roues dentées engrenées comptent 18 et 24 dents. Après combien de tours de chacune retrouve-t-on la position initiale ?

Exercice 4 - Nombres premiers entre eux et fractions irréductibles

Deux entiers sont PREMIERS ENTRE EUX lorsque leur PGCD vaut 1, c'est-à-dire lorsque leur seul diviseur commun positif est 1. Attention : cela ne signifie pas qu'ils sont premiers.

1. Les entiers 35 et 24 sont-ils premiers entre eux ? Sont-ils premiers ?
2. Rendre irréductible la fraction $\frac{1071}{462}$.
3. Démontrer que pour tout entier n , la fraction $\frac{n}{n+1}$ est irréductible.

Exercice 5 - Coefficients de Bézout par remontée

L'identité de Bézout affirme qu'il existe toujours des entiers u et v tels que $au + bv = \text{PGCD}(a; b)$. On les obtient en REMONTANT l'algorithme d'Euclide : on part de l'avant-dernière ligne et on substitue les restes de proche en proche.

1. Écrire les divisions successives de l'algorithme d'Euclide pour 1071 et 462.
2. Remonter l'algorithme pour trouver u et v tels que $1071u + 462v = 21$.
3. Vérifier le résultat.

Exercice 6 - PGCD d'expressions dépendant de n

Pour un PGCD dépendant d'un entier n , la méthode est toujours la même : trouver une combinaison linéaire des deux expressions qui élimine n . Tout diviseur commun divise alors cette constante.

1. Démontrer que $2n + 1$ et $3n + 2$ sont premiers entre eux pour tout entier n .
2. Déterminer les valeurs possibles de $\text{PGCD}(n; n + 2)$.
3. En déduire que la fraction $\frac{2n+1}{3n+2}$ est toujours irréductible.

Exercice 7 - Théorème de Bézout

Le théorème de Bézout est une équivalence : a et b sont premiers entre eux SI ET SEULEMENT S'IL existe des entiers u et v tels que $au + bv = 1$. Le sens direct vient de l'identité de Bézout ; le sens réciproque est celui qu'on utilise pour démontrer.

1. Déterminer u et v tels que $7u + 12v = 1$.
2. Démontrer le sens réciproque : si $au + bv = 1$ pour certains entiers u et v , alors $\text{PGCD}(a; b) = 1$.
3. En déduire que $2n + 1$ et $3n + 2$ sont premiers entre eux (exercice 6), en une ligne.

Exercice 8 - Inverse modulaire

Modulo n , un entier a admet un INVERSE — un entier a' tel que $aa' \equiv 1 [n]$ — si et seulement si a et n sont premiers entre eux. Bézout en fournit la preuve et le calcul.

1. Justifier que 7 admet un inverse modulo 12, et le déterminer à l'aide de l'exercice

- 7.
2. Déterminer l'inverse de 5 modulo 26.
3. Démontrer que si a et n ne sont pas premiers entre eux, a n'a pas d'inverse modulo n .

Exercice 9 - Théorème de Gauss

Le théorème de Gauss énonce : si a divise bc et si a et b sont premiers entre eux, alors a divise c . L'hypothèse de primalité entre a et b est indispensable.

1. Démontrer le théorème de Gauss à l'aide de l'identité de Bézout.
2. Montrer par un contre-exemple que l'hypothèse « a et b premiers entre eux » ne peut pas être supprimée.
3. Application : déterminer les entiers c tels que $7 \mid 5c$.

Exercice 10 - Équation diophantienne : le cas général

Une équation diophantienne $ax + by = c$ se résout en trois temps : condition d'existence, solution particulière, puis solution générale obtenue par le théorème de Gauss. On résout $(E) : 2x + 3y = 5$, puis $12x + 18y = 30$.

1. Justifier que (E) admet des solutions, et en trouver une évidente.
2. Résoudre (E) dans $\mathbb{Z}^2$.
3. Résoudre $12x + 18y = 30$.

Exercice 11 - Équation diophantienne avec coefficients de signes opposés

On résout $(E) : 7x - 12y = 5$ dans $\mathbb{Z}^2$. Le signe négatif ne change rien à la méthode, mais il modifie l'allure des solutions.

1. Justifier l'existence de solutions et en déterminer une particulière.
2. Résoudre (E) dans $\mathbb{Z}^2$.
3. Déterminer les solutions telles que $0 \leq x \leq 50$.

Exercice 12 - Un problème concret

Un libraire vend deux formats de carnets : les petits à 7 € et les grands à 12 €. Une matinée, sa recette sur ces carnets s'élève à 100 €. On cherche combien il a vendu de carnets de chaque sorte.

1. Mettre le problème en équation, en précisant les contraintes sur les inconnues.
2. Résoudre l'équation dans $\mathbb{Z}^2$.
3. Déterminer toutes les solutions possibles pour le libraire.

Exercice 13 - PGCD avec paramètre : discussion complète

On étudie $d_n = \text{PGCD}(n + 2 ; 3n + 1)$ selon les valeurs de l'entier naturel n .

1. Démontrer que d_n divise 5.
2. Déterminer les valeurs de n pour lesquelles $d_n = 5$.

3. Conclure par une discussion complète, et vérifier sur deux exemples.

Exercice 14 - Système de congruences par Bézout

Le chapitre précédent résolvait les systèmes de congruences par balayage. Avec un inverse modulaire, la résolution devient directe. On cherche les entiers x tels que $x \equiv 3 [7]$ et $x \equiv 5 [11]$.

1. Traduire la première condition, puis reporter dans la seconde.
2. Résoudre la congruence obtenue à l'aide d'un inverse modulaire.
3. Conclure et vérifier.

Exercice 15 - Fractions irréductibles et simplification

Une fraction $\frac{a}{b}$ est irréductible lorsque a et b sont premiers entre eux. Décider si une fraction dépendant de n est irréductible revient donc à un calcul de PGCD avec paramètre.

1. La fraction $\frac{n+1}{2n+3}$ est-elle irréductible pour tout entier naturel n ?
2. Même question pour $\frac{3n+4}{n+1}$.
3. Pour quelles valeurs de n la fraction $\frac{2n+3}{5n+2}$ est-elle réductible ?

Exercice 16 - Multiples communs et cycles

Trois phares émettent un éclat respectivement toutes les 15, 18 et 24 secondes. Ils viennent d'émettre simultanément à l'instant $t = 0$.

1. Dans combien de temps les deux premiers phares seront-ils à nouveau synchrones ?
2. Dans combien de temps les trois le seront-ils ?
3. Combien de fois les trois phares seront-ils synchrones au cours d'une heure (instant initial exclu) ?

Exercice 17 - Solutions positives d'une équation diophantienne

On cherche tous les couples d'entiers NATURELS $(x; y)$ vérifiant $23x + 17y = 1000$. La résolution générale ne suffit pas : il faut ensuite encadrer le paramètre.

1. Déterminer, par l'algorithme d'Euclide, des entiers u et v tels que $23u + 17v = 1$.
2. En déduire une solution particulière puis la solution générale de l'équation.
3. Déterminer toutes les solutions en entiers naturels.

Exercice 18 - Résoudre une congruence avec un grand module

On résout $17x \equiv 5 [26]$. Le balayage des 26 restes fonctionnerait, mais l'inverse modulaire donne la réponse en trois lignes — et reste praticable pour des modules bien plus grands.

1. Justifier que l'équation admet une unique solution modulo 26.

2. Déterminer l'inverse de 17 modulo 26 par l'algorithme d'Euclide.
3. Résoudre l'équation et vérifier.

Exercice 19 - Problème type bac : congruences et dénombrement

On cherche les entiers naturels n vérifiant simultanément $n \equiv 1 [5]$ et $n \equiv 3 [8]$.

1. Déterminer une solution particulière.
2. Démontrer que l'ensemble des solutions est $n \equiv 11 [40]$.
3. Déterminer le nombre de solutions comprises entre 1 et 1000, ainsi que la plus grande.

Exercice 20 - Problème de synthèse : Bézout et déchiffrement

On considère l'équation $(E) : 11x - 26y = 1$, d'inconnues entières x et y . Elle va servir à déchiffrer un code affine où chaque lettre de rang x (avec $A = 0, \dots, Z = 25$) est codée par la lettre de rang $y \equiv 11x + 4 [26]$.

1. Justifier que (E) admet des solutions, et en déterminer une par l'algorithme d'Euclide.
2. Résoudre (E) dans $\mathbb{Z}^2$.
3. En déduire l'inverse de 11 modulo 26, puis résoudre $11x \equiv 7 [26]$.
4. Établir la formule de déchiffrement du code affine, et décoder la lettre G .

Corrigés détaillés

Les corrections des 20 exercices, dans l'ordre des énoncés.

Correction de l'exercice 1 - PGCD par les diviseurs et par la décomposition

Diviseurs positifs de 84 : 1, 2, 3, 4, 6, 7, 12, 14, 21, 28, 42, 84.

Diviseurs positifs de 60 : 1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60.

Les diviseurs COMMUNS sont ceux qui figurent dans les deux listes : 1, 2, 3, 4, 6, 12.

Le plus grand est 12 : donc $\text{PGCD}(84; 60) = 12$.

On remarque au passage que tous les diviseurs communs divisent 12 : c'est une propriété générale du PGCD, et non un hasard sur cet exemple.

Décomposition en facteurs premiers : $84 = 2^2 \times 3 \times 7$ et $60 = 2^2 \times 3 \times 5$.

Le PGCD se lit en prenant chaque facteur premier commun avec le plus PETIT exposant : $2^2 \times 3^1 = 12$ ✓.

Le facteur 7 n'apparaît que dans 84 et le facteur 5 que dans 60 : ils sont absents du PGCD.

Pour le PPCM, on prend au contraire chaque facteur premier présent avec le plus GRAND exposant : $2^2 \times 3 \times 5 \times 7 = 420$.

Contrôle par la relation fondamentale : $\text{PGCD} \times \text{PPCM} = 12 \times 420 = 5040$, et $84 \times 60 = 5040$ ✓.

Réponse. Diviseurs communs : 1, 2, 3, 4, 6, 12 · $\text{PGCD}(84; 60) = 12$ · $84 = 2^2 \times 3 \times 7$ et $60 = 2^2 \times 3 \times 5$ · $\text{PPCM}(84; 60) = 420$.

Rappel de cours. Par décomposition : PGCD = facteurs communs au plus petit exposant, PPCM = tous les facteurs au plus grand exposant. Et toujours $\text{PGCD}(a; b) \times \text{PPCM}(a; b) = ab$ pour $a, b > 0$.

Erreur fréquente. Prendre le plus grand exposant pour le PGCD. C'est l'inverse : le PGCD doit diviser les DEUX nombres, il prend donc le plus petit exposant.

Correction de l'exercice 2 - Algorithme d'Euclide

Première division : $1071 = 2 \times 462 + 147$.

On remplace le couple (1071 ; 462) par (462 ; 147) : $462 = 3 \times 147 + 21$.

Nouveau couple (147 ; 21) : $147 = 7 \times 21 + 0$.

Le reste est nul : le dernier reste NON NUL est 21. Donc $\text{PGCD}(1071; 462) = 21$.

Contrôle : $1071 = 21 \times 51$ et $462 = 21 \times 22$ ✓, et 51 et 22 n'ont plus de diviseur commun.

Deuxième calcul : $255 = 2 \times 108 + 39$; $108 = 2 \times 39 + 30$; $39 = 1 \times 30 + 9$.

On poursuit : $30 = 3 \times 9 + 3$; $9 = 3 \times 3 + 0$.

Le dernier reste non nul est 3 : $\text{PGCD}(255; 108) = 3$.

Contrôle : $255 = 3 \times 85$ et $108 = 3 \times 36$ ✓.

Justification de la propriété. Soit $a = bq + r$. Montrons que les diviseurs communs de a et b sont exactement ceux de b et r .

Si d divise a et b , alors d divise la combinaison $a - bq = r$: donc d divise b et r .

Réciproquement, si d divise b et r , alors d divise $bq + r = a$: donc d divise a et b .

Les deux couples ont donc les MÊMES diviseurs communs, donc le même plus grand : l'algorithme est légitime. Et comme les restes décroissent strictement, il se termine toujours.

Réponse. $\text{PGCD}(1071; 462) = 21 \cdot \text{PGCD}(255; 108) = 3 \cdot$ la propriété vient de ce que $d \mid a$ et $d \mid b$ équivaut à $d \mid b$ et $d \mid r$, via $r = a - bq$.

Rappel de cours. Algorithme d'Euclide : on divise, on décale, on recommence. Le PGCD est le DERNIER RESTE NON NUL. La suite des restes est strictement décroissante, donc l'algorithme s'arrête.

Erreur fréquente. Annoncer 0 comme PGCD parce que le dernier reste est nul. C'est le dernier reste NON NUL qu'on retient.

Correction de l'exercice 3 - PGCD, PPCM et leur relation

On a vu $\text{PGCD}(1071; 462) = 21$ à l'exercice précédent.

Par la relation $\text{PGCD} \times \text{PPCM} = ab$, on obtient $\text{PPCM} = \frac{1071 \times 462}{21}$.

On simplifie avant de multiplier : $\frac{462}{21} = 22$, donc $\text{PPCM} = 1071 \times 22 = 23\,562$.

Contrôle : $23\,562 = 1071 \times 22$ ✓ et $23\,562 = 462 \times 51$ ✓ : c'est bien un multiple commun.

Deuxième situation : les instants de clignotement du premier feu sont les multiples de 12, ceux du second les multiples de 18.

Ils coïncident aux multiples COMMUNS, et la première coïncidence est le PPCM.

$\text{PGCD}(12; 18) = 6$, donc $\text{PPCM}(12; 18) = \frac{12 \times 18}{6} = 36$.

Les deux feux clignoteront à nouveau ensemble dans 36 secondes.

Troisième situation : la position initiale est retrouvée quand un même nombre de dents est passé, multiple de 18 et de 24.

$\text{PGCD}(18; 24) = 6$, donc $\text{PPCM}(18; 24) = \frac{18 \times 24}{6} = 72$.

Il faut donc que 72 dents défilent. La première roue fait $\frac{72}{18} = 4$ tours, la seconde $\frac{72}{24} = 3$ tours.

Contrôle de cohérence : la roue qui a le moins de dents tourne plus vite, et c'est bien celle de 18 dents qui fait le plus de tours ✓.

Réponse. $\text{PGCD}(1071; 462) = 21$ et $\text{PPCM} = 23\,562$: les feux coïncident toutes les 36 secondes : les roues retrouvent leur position après 4 tours de la première et 3 tours de la seconde.

Rappel de cours. $\text{PGCD}(a; b) \times \text{PPCM}(a; b) = ab$. Une question de « coïncidence » ou de « retour à la position de départ » se traduit toujours par un PPCM.

Erreur fréquente. Calculer $a \times b$ puis diviser. On simplifie AVANT de multiplier, sinon les nombres explosent inutilement.

Correction de l'exercice 4 - Nombres premiers entre eux et fractions irréductibles

$35 = 5 \times 7$ et $24 = 2^3 \times 3$. Aucun facteur premier commun, donc $\text{PGCD}(35; 24) = 1$: ils sont premiers entre eux.

En revanche, ni 35 ni 24 n'est un nombre PREMIER : chacun a des diviseurs autres que 1 et lui-même.

La distinction est essentielle : « premiers entre eux » est une propriété du COUPLE, « premier » est une propriété d'un seul nombre.

Pour la fraction, on divise numérateur et dénominateur par leur PGCD, qui vaut 21 (exercice 2).

$$\frac{1071}{462} = \frac{1071 \div 21}{462 \div 21} = \frac{51}{22}.$$

Vérification de l'irréductibilité : $51 = 3 \times 17$ et $22 = 2 \times 11$. Aucun facteur commun, donc $\text{PGCD}(51; 22) = 1$ ✓ : la fraction est bien irréductible.

Simplifier par le PGCD garantit d'aboutir en une seule étape : c'est ce qui distingue cette méthode des simplifications successives « au jugé ».

Troisième question : soit d un diviseur commun de n et $n + 1$.

Alors d divise la différence $(n + 1) - n = 1$.

Or les seuls diviseurs de 1 sont 1 et -1 . Donc $\text{PGCD}(n; n + 1) = 1$: deux entiers consécutifs sont toujours premiers entre eux.

La fraction $\frac{n}{n+1}$ est donc irréductible pour tout entier n , quelle que soit sa taille.

Ce raisonnement — faire apparaître une petite combinaison linéaire — est le modèle de tous les exercices de PGCD avec paramètre (voir l'exercice 13).

Réponse. 35 et 24 sont premiers entre eux mais ne sont pas premiers. $\frac{1071}{462} = \frac{51}{22}$, irréductible. $d \mid n$ et $d \mid n + 1$ entraînent $d \mid 1$, donc $\frac{n}{n+1}$ est toujours irréductible.

Rappel de cours. a et b premiers entre eux $\Leftrightarrow \text{PGCD}(a; b) = 1$. Pour prouver qu'un PGCD vaut 1, on montre qu'un diviseur commun divise une combinaison linéaire égale à 1.

Erreur fréquente. Confondre « premiers entre eux » et « premiers ». 35 et 24 sont premiers entre eux sans qu'aucun des deux ne soit premier.

Correction de l'exercice 5 - Coefficients de Bézout par remontée

Les divisions ont été faites à l'exercice 2. On les réécrit en isolant à chaque fois le RESTE, ce qui prépare la remontée.

$$1071 = 2 \times 462 + 147, \text{ donc } 147 = 1071 - 2 \times 462.$$

$$462 = 3 \times 147 + 21, \text{ donc } 21 = 462 - 3 \times 147.$$

$$147 = 7 \times 21 + 0 : \text{c'est la ligne d'arrêt, elle ne sert pas dans la remontée.}$$

Remontée. On part de la dernière ligne utile, celle qui donne le PGCD :
 $21 = 462 - 3 \times 147.$

$$\text{On y remplace } 147 \text{ par son expression : } 21 = 462 - 3 \times (1071 - 2 \times 462).$$

$$\text{On développe SANS calculer les produits par } 1071 \text{ et } 462, \text{ qu'on garde comme des blocs : } 21 = 462 - 3 \times 1071 + 6 \times 462.$$

$$\text{On regroupe : } 21 = -3 \times 1071 + 7 \times 462.$$

$$\text{On lit les coefficients : } u = -3 \text{ et } v = 7.$$

Vérification : $-3 \times 1071 = -3213$ et $7 \times 462 = 3234$. La somme vaut $-3213 + 3234 = 21$ ✓.

Remarque : le couple $(u; v)$ n'est pas unique. En ajoutant 462 à u et en retranchant 1071 à v (divisés par le PGCD), on obtient d'autres solutions — c'est ce que formalisera l'exercice 10.

Conseil de rédaction : ne jamais effectuer les produits pendant la remontée. C'est en gardant 1071 et 462 apparents qu'on lit les coefficients à la fin.

Réponse. $147 = 1071 - 2 \times 462$ et $21 = 462 - 3 \times 147$ · en substituant :
 $21 = -3 \times 1071 + 7 \times 462$, donc $u = -3$ et $v = 7$ · vérification : $-3213 + 3234 = 21$ ✓.

Rappel de cours. Identité de Bézout : il existe u, v entiers tels que $au + bv = \text{PGCD}(a; b)$. On les obtient en remontant l'algorithme d'Euclide, en gardant a et b sous forme de blocs.

Erreur fréquente. Effectuer les multiplications au fil de la remontée. On perd alors de vue les coefficients de a et de b , qui sont précisément le résultat cherché.

Correction de l'exercice 6 - PGCD d'expressions dépendant de n

Soit d un diviseur commun de $2n + 1$ et $3n + 2$. Cherchons une combinaison qui fasse disparaître n .

On multiplie la première expression par 3 et la seconde par 2 : $3(2n + 1) = 6n + 3$ et $2(3n + 2) = 6n + 4$.

d divise ces deux quantités, donc leur différence :

$$3(2n + 1) - 2(3n + 2) = (6n + 3) - (6n + 4) = -1.$$

Donc d divise -1 , c'est-à-dire $d = 1$ (en se limitant aux diviseurs positifs).

Le PGCD vaut donc 1 : les deux expressions sont premières entre elles pour TOUT entier n .

Contrôle sur un exemple : $n = 5$ donne 11 et 17, effectivement premiers entre eux ✓.

Deuxième question : soit d un diviseur commun de n et $n + 2$. Alors d divise $(n + 2) - n = 2$.

Les diviseurs positifs de 2 sont 1 et 2 : le PGCD vaut donc 1 ou 2.

Il vaut 2 exactement quand 2 divise n et $n + 2$, c'est-à-dire quand n est PAIR.

Il vaut 1 quand n est impair. Contrôle : $n = 4$ donne $\text{PGCD}(4; 6) = 2$ ✓ ; $n = 5$ donne $\text{PGCD}(5; 7) = 1$ ✓.

Troisième question : la fraction $\frac{2n+1}{3n+2}$ a un numérateur et un dénominateur premiers entre eux d'après la question 1.

Elle est donc irréductible pour tout entier n , sans aucune exception à discuter.

Précision : il faut tout de même $3n + 2 \neq 0$, ce qui est automatique pour n entier puisque $-\frac{2}{3}$ n'est pas entier.

Réponse. $3(2n + 1) - 2(3n + 2) = -1$, donc $\text{PGCD}(2n + 1; 3n + 2) = 1$ pour tout n ·
 $\text{PGCD}(n; n + 2)$ vaut 2 si n est pair, 1 sinon · la fraction $\frac{2n+1}{3n+2}$ est toujours irréductible.

Rappel de cours. Méthode : « d divise A et B , donc d divise $\alpha A + \beta B$ ». On choisit α et β pour éliminer n ; le PGCD divise alors la constante obtenue.

Erreur fréquente. Conclure que le PGCD VAUT la constante trouvée. Il la DIVISE seulement : dans la question 2, il vaut 1 ou 2 selon la parité de n .

Correction de l'exercice 7 - Théorème de Bézout

On peut procéder par l'algorithme d'Euclide, mais les nombres sont assez petits pour un essai direct.

On cherche un multiple de 12 qui dépasse d'exactly 1 un multiple de 7 : $12 \times 3 = 36$ et $7 \times 5 = 35$.

D'où $36 - 35 = 1$, c'est-à-dire $7 \times (-5) + 12 \times 3 = 1$.

Les coefficients $u = -5$ et $v = 3$ conviennent. Vérification : $-35 + 36 = 1$ ✓.

Démonstration du sens réciproque. Supposons qu'il existe u et v entiers tels que $au + bv = 1$.

Soit d un diviseur commun positif de a et b . Alors d divise toute combinaison linéaire entière de a et b , en particulier $au + bv$.

Donc d divise 1, ce qui impose $d = 1$.

Le seul diviseur commun positif de a et b est donc 1 : ils sont premiers entre eux.

Attention à la portée du théorème : l'existence d'une combinaison égale à 1 est une condition SUFFISANTE, et c'est ce qui la rend si commode. Si la combinaison vaut 5, on ne peut rien conclure directement.

Application immédiate : on a établi à l'exercice 6 que $3(2n + 1) - 2(3n + 2) = -1$.

En changeant les signes : $(-3)(2n + 1) + 2(3n + 2) = 1$.

C'est une combinaison linéaire à coefficients entiers égale à 1 : par le théorème de Bézout, $2n + 1$ et $3n + 2$ sont premiers entre eux ✓.

On voit ici l'intérêt du théorème : il transforme un raisonnement sur les diviseurs en une simple exhibition de deux coefficients.

Réponse. $7 \times (-5) + 12 \times 3 = 1$ · si $au + bv = 1$, tout diviseur commun divise 1, donc le PGCD vaut 1 · $(-3)(2n + 1) + 2(3n + 2) = 1$ prouve directement que ces deux nombres sont premiers entre eux.

Rappel de cours. Théorème de Bézout : $\text{PGCD}(a; b) = 1 \Leftrightarrow \exists u, v \in \mathbb{Z}, au + bv = 1$. Une seule combinaison égale à 1 suffit à conclure.

Erreur fréquente. Conclure d'une combinaison $au + bv = 5$ que le PGCD vaut 5. Il divise 5 seulement : il pourrait valoir 1.

Correction de l'exercice 8 - Inverse modulaire

$\text{PGCD}(7; 12) = 1$, donc 7 est inversible modulo 12.

L'exercice 7 a donné $7 \times (-5) + 12 \times 3 = 1$. On réduit cette égalité modulo 12 : le terme 12×3 disparaît.

Il reste $7 \times (-5) \equiv 1 [12]$. L'inverse est donc -5 , qu'on préfère écrire entre 0 et 11 : $-5 \equiv 7 [12]$.

L'inverse de 7 modulo 12 est donc 7 lui-même. Vérification : $7 \times 7 = 49 = 48 + 1 \equiv 1 [12]$ ✓.

Deuxième question : $\text{PGCD}(5; 26) = 1$, l'inverse existe. On cherche une combinaison $5u + 26v = 1$.

Par essais guidés : $5 \times 21 = 105$ et $26 \times 4 = 104$, donc $5 \times 21 - 26 \times 4 = 1$.

En réduisant modulo 26 : $5 \times 21 \equiv 1 [26]$. L'inverse de 5 modulo 26 est 21.

Vérification : $105 = 26 \times 4 + 1$ ✓. C'est le nombre qui servait déjà au déchiffrement affine du chapitre précédent — on sait maintenant d'où il vient.

Troisième question. Supposons que a ait un inverse a' modulo n : $aa' \equiv 1 [n]$.

Cela signifie que n divise $aa' - 1$, donc qu'il existe un entier k tel que $aa' - 1 = kn$.

En réorganisant : $aa' - kn = 1$, c'est-à-dire $a \times a' + n \times (-k) = 1$.

Par le théorème de Bézout, a et n sont donc premiers entre eux.

Par contraposée : si a et n ne sont pas premiers entre eux, a n'a pas d'inverse modulo n .

Illustration : modulo 26, le nombre 13 n'a pas d'inverse (leur PGCD vaut 13) — c'est exactement pourquoi 13 était inutilisable comme coefficient de chiffrement.

Réponse. Inverse de 7 modulo 12 : 7 (car $49 = 48 + 1$) · inverse de 5 modulo 26 : 21 (car $105 = 104 + 1$) · a inversible modulo $n \Leftrightarrow \text{PGCD}(a; n) = 1$.

Rappel de cours. Pour inverser a modulo n : écrire $au + nv = 1$ par Bézout, puis réduire modulo n — il reste $au \equiv 1$, donc u est l'inverse.

Erreur fréquente. Chercher un inverse sans vérifier le PGCD. Modulo 26, les nombres pairs et 13 n'en ont aucun : le calcul ne peut pas aboutir.

Correction de l'exercice 9 - Théorème de Gauss

Hypothèses : $a \mid bc$ et $\text{PGCD}(a; b) = 1$. On veut montrer que $a \mid c$.

Par le théorème de Bézout, il existe des entiers u et v tels que $au + bv = 1$.

On multiplie cette égalité par c : $auc + bvc = c$.

Examinons les deux termes du membre de gauche. Le premier, auc , est manifestement divisible par a .

Le second, $bvc = (bc)v$, est divisible par a puisque $a \mid bc$ par hypothèse.

a divise donc la somme de ces deux termes, c'est-à-dire c . Le théorème est démontré.

Contre-exemple : prenons $a = 6$, $b = 4$ et $c = 3$. Alors $bc = 12$, et $6 \mid 12$ ✓.

Pourtant 6 ne divise pas 3. L'implication est donc fausse ici.

Ce qui manque : $\text{PGCD}(6; 4) = 2 \neq 1$. L'hypothèse de Gauss n'est pas vérifiée, et la conclusion tombe.

Application : on cherche les c tels que $7 \mid 5c$.

Or $\text{PGCD}(7; 5) = 1$: les deux nombres sont premiers entre eux.

Par le théorème de Gauss (avec $a = 7$, $b = 5$), on en déduit $7 \mid c$.

Réciproquement, si $7 \mid c$ alors $7 \mid 5c$. Les entiers cherchés sont donc exactement les MULTIPLES DE 7.

Contrôle : $c = 14$ donne $5c = 70 = 7 \times 10$ ✓ ; $c = 3$ donne $5c = 15$, non divisible par 7 ✓.

Réponse. Démonstration : multiplier $au + bv = 1$ par c , les deux termes obtenus sont divisibles par a · contre-exemple : $6 \mid 4 \times 3$ mais $6 \nmid 3$, car $\text{PGCD}(6; 4) = 2 \cdot 7 \nmid 5c \Leftrightarrow 7 \nmid c$.

Rappel de cours. Théorème de Gauss : $a \mid bc$ et $\text{PGCD}(a; b) = 1 \Rightarrow a \mid c$. Corollaire utile : si b et c premiers entre eux divisent tous deux n , alors $bc \mid n$.

Erreur fréquente. Appliquer Gauss sans vérifier la primalité. C'est précisément l'hypothèse qui fait tout le travail, comme le montre le contre-exemple.

Correction de l'exercice 10 - Équation diophantienne : le cas général

$\text{PGCD}(2; 3) = 1$, et 1 divise 5 : l'équation admet donc des solutions entières.

Solution particulière évidente : $x_0 = 1$ et $y_0 = 1$, puisque $2 + 3 = 5$ ✓.

Passons au cas général. Soit $(x; y)$ une solution quelconque. On écrit les deux égalités : $2x + 3y = 5$ et $2 \times 1 + 3 \times 1 = 5$.

En soustrayant : $2(x - 1) + 3(y - 1) = 0$, c'est-à-dire $2(x - 1) = -3(y - 1)$.

Donc 3 divise $2(x - 1)$. Or $\text{PGCD}(3; 2) = 1$, donc par le THÉORÈME DE GAUSS, 3 divise $x - 1$.

Il existe donc un entier k tel que $x - 1 = 3k$, soit $x = 1 + 3k$.

En reportant : $2 \times 3k = -3(y - 1)$, donc $6k = -3(y - 1)$ et $y - 1 = -2k$, soit $y = 1 - 2k$.

Réciproquement, pour tout entier k : $2(1 + 3k) + 3(1 - 2k) = 2 + 6k + 3 - 6k = 5$ ✓.

L'ensemble des solutions est donc $\{(1 + 3k ; 1 - 2k), k \in \mathbb{Z}\}$.

Deuxième équation : $\text{PGCD}(12 ; 18) = 6$, et 6 divise 30 : il y a des solutions.

On DIVISE toute l'équation par 6 : $2x + 3y = 5$. C'est exactement (E).

Les solutions sont donc les mêmes : $x = 1 + 3k$ et $y = 1 - 2k$, pour $k \in \mathbb{Z}$.

Contrôle : $k = 2$ donne $(7 ; -3)$, et $12 \times 7 + 18 \times (-3) = 84 - 54 = 30$ ✓.

Cette simplification préalable est systématique : elle ramène toujours au cas où les coefficients sont premiers entre eux, seul cas où Gauss s'applique.

Réponse. (E) a des solutions car $\text{PGCD}(2 ; 3) = 1$ divise 5 · solution particulière $(1 ; 1)$ · solutions : $x = 1 + 3k, y = 1 - 2k, k \in \mathbb{Z}$ · $12x + 18y = 30$ se ramène à (E) après division par 6, mêmes solutions.

Rappel de cours. $ax + by = c$ a des solutions $\Leftrightarrow \text{PGCD}(a ; b) \mid c$. Méthode : simplifier par le PGCD, trouver une solution particulière, soustraire les deux égalités, appliquer Gauss.

Erreur fréquente. Oublier la réciproque. La méthode donne les solutions POSSIBLES ; il faut vérifier que toutes conviennent, ce qui se fait en une ligne de calcul.

Correction de l'exercice 11 - Équation diophantienne avec coefficients de signes opposés

$\text{PGCD}(7 ; 12) = 1$ (exercice 7), et 1 divise 5 : il y a des solutions.

Pour une solution particulière, on part de l'identité de Bézout trouvée à l'exercice 7 : $7 \times (-5) + 12 \times 3 = 1$.

On la réécrit sous la forme de (E) : $7 \times (-5) - 12 \times (-3) = 1$.

En multipliant par 5 : $7 \times (-25) - 12 \times (-15) = 5$. Le couple $(-25 ; -15)$ est donc solution.

On peut chercher plus simple par essais : $x = -1$ donne $-7 - 12y = 5$, soit $-12y = 12$ et $y = -1$.

Le couple $(-1 ; -1)$ convient : $7 \times (-1) - 12 \times (-1) = -7 + 12 = 5$ ✓. On le préfère, les nombres étant plus petits.

Cas général : soit $(x ; y)$ solution. En soustrayant l'égalité particulière : $7(x + 1) - 12(y + 1) = 0$, soit $7(x + 1) = 12(y + 1)$.

Donc 12 divise $7(x + 1)$. Comme $\text{PGCD}(12 ; 7) = 1$, le théorème de Gauss donne $12 \mid x + 1$.

Il existe donc k entier tel que $x + 1 = 12k$, soit $x = -1 + 12k$.

En reportant : $7 \times 12k = 12(y + 1)$, donc $y + 1 = 7k$ et $y = -1 + 7k$.

Réciproque : $7(-1 + 12k) - 12(-1 + 7k) = -7 + 84k + 12 - 84k = 5$ ✓ pour tout k .

Les solutions sont donc $\{(-1 + 12k ; -1 + 7k), k \in \mathbb{Z}\}$.

Dernière question : on impose $0 \leq -1 + 12k \leq 50$, soit $1 \leq 12k \leq 51$, c'est-à-dire $\frac{1}{12} \leq k \leq \frac{51}{12} = 4,25$.

Les entiers k convenables sont 1, 2, 3, 4, qui donnent les couples $(11 ; 6)$, $(23 ; 13)$, $(35 ; 20)$ et $(47 ; 27)$.

Contrôle sur le premier : $7 \times 11 - 12 \times 6 = 77 - 72 = 5$ ✓.

Réponse. Solution particulière : $(-1 ; -1)$ · solutions générales : $x = -1 + 12k, y = -1 + 7k, k \in \mathbb{Z}$ · pour $0 \leq x \leq 50$: $(11 ; 6)$, $(23 ; 13)$, $(35 ; 20)$, $(47 ; 27)$.

Rappel de cours. Dans $ax + by = c$ avec a et b premiers entre eux, le pas des solutions est toujours b pour x et a pour y (au signe près) : c'est la structure imposée par Gauss.

Erreur fréquente. Chercher une solution particulière uniquement par Bézout. Un essai

direct sur de petits nombres est souvent plus rapide, et donne des coefficients plus maniables.

Correction de l'exercice 12 - Un problème concret

Notons x le nombre de petits carnets et y le nombre de grands carnets vendus.

La recette s'écrit $7x + 12y = 100$. Les contraintes sont $x \geq 0$ et $y \geq 0$, avec x et y ENTIERS — on ne vend pas un demi-carnet.

C'est ce qui fait de ce problème une équation diophantienne, et non une simple équation à deux inconnues.

Existence : $\text{PGCD}(7; 12) = 1$ divise 100, il y a des solutions entières.

Solution particulière : à partir de $7 \times (-5) + 12 \times 3 = 1$, on multiplie par 100 :
 $7 \times (-500) + 12 \times 300 = 100$.

Le couple $(-500; 300)$ est solution — mathématiquement correct, mais évidemment sans signification commerciale.

Cas général : en soustrayant, $7(x + 500) + 12(y - 300) = 0$, soit $7(x + 500) = -12(y - 300)$.
 12 divise $7(x + 500)$ et $\text{PGCD}(12; 7) = 1$, donc par Gauss $12 \mid x + 500$: $x = -500 + 12k$.

En reportant : $y = 300 - 7k$. Les solutions entières sont donc
 $\{(-500 + 12k; 300 - 7k), k \in \mathbb{Z}\}$.

Contraintes de positivité. $x \geq 0$ donne $12k \geq 500$, soit $k \geq 41,67$, donc $k \geq 42$.

$y \geq 0$ donne $7k \leq 300$, soit $k \leq 42,86$, donc $k \leq 42$.

Les deux contraintes imposent $k = 42$, et une seule possibilité.

Pour $k = 42$: $x = -500 + 504 = 4$ et $y = 300 - 294 = 6$.

Le libraire a donc vendu 4 petits carnets et 6 grands. Vérification :
 $7 \times 4 + 12 \times 6 = 28 + 72 = 100$ ✓.

La solution est UNIQUE, ce qui n'a rien d'automatique : avec une recette de 200 €, il y aurait plusieurs répartitions possibles.

Réponse. $7x + 12y = 100$ avec x, y entiers positifs · solutions entières : $x = -500 + 12k$,
 $y = 300 - 7k$ · seule $k = 42$ respecte les contraintes : 4 petits carnets et 6 grands.

Rappel de cours. Dans un problème concret, la résolution comporte deux étages :
 d'abord toutes les solutions ENTIÈRES, puis le filtrage par les contraintes de positivité,
 qui donne un intervalle d'entiers pour k .

Erreur fréquente. Rejeter la solution particulière parce qu'elle est négative. Elle sert
 d'ancrage au calcul général : les contraintes ne s'appliquent qu'à la fin.

Correction de l'exercice 13 - PGCD avec paramètre : discussion complète

Soit d un diviseur commun de $n + 2$ et $3n + 1$. On cherche une combinaison éliminant n .

On multiplie la première expression par 3 : $3(n + 2) = 3n + 6$.

d divise $3n + 6$ et $3n + 1$, donc leur différence : $(3n + 6) - (3n + 1) = 5$.

Donc $d \mid 5$. Comme 5 est premier, ses diviseurs positifs sont 1 et 5 : d_n vaut donc 1 ou 5.

Deuxième question : $d_n = 5$ exige que 5 divise $n + 2$, c'est-à-dire $n + 2 \equiv 0 [5]$, soit
 $n \equiv -2 \equiv 3 [5]$.

Vérifions que cette condition est aussi SUFFISANTE : si $n \equiv 3 [5]$, alors
 $3n + 1 \equiv 9 + 1 = 10 \equiv 0 [5]$.

Dans ce cas, 5 divise les deux expressions, donc $d_n = 5$ (puisque d_n ne peut valoir que 1

ou 5).

Discussion complète : $d_n = 5$ si $n \equiv 3 [5]$, et $d_n = 1$ sinon.

Premier contrôle, $n = 3$: les expressions valent 5 et 10, de PGCD 5 ✓, et $3 \equiv 3 [5]$ ✓.

Second contrôle, $n = 4$: les expressions valent 6 et 13, de PGCD 1 ✓, et $4 \not\equiv 3 [5]$ ✓.

Troisième contrôle, $n = 8$: les expressions valent 10 et 25, de PGCD 5 ✓, et $8 = 5 + 3 \equiv 3 [5]$ ✓.

Conséquence utile : la fraction $\frac{n+2}{3n+1}$ est irréductible sauf quand $n \equiv 3 [5]$, auquel cas elle se simplifie par 5.

Réponse. $3(n+2) - (3n+1) = 5$, donc $d_n \mid 5$ et $d_n \in \{1; 5\}$ · $d_n = 5 \Leftrightarrow n \equiv 3 [5]$ · $d_n = 1$ dans tous les autres cas.

Rappel de cours. Discussion type : (1) montrer que le PGCD divise une constante c ; (2) pour chaque diviseur de c , chercher la condition de congruence sur n ; (3) vérifier qu'elle est suffisante.

Erreur fréquente. S'arrêter à « d_n divise 5 ». Il reste à déterminer QUAND chaque valeur est atteinte : c'est la partie où la congruence intervient.

Correction de l'exercice 14 - Système de congruences par Bézout

La condition $x \equiv 3 [7]$ signifie qu'il existe un entier k tel que $x = 3 + 7k$.

On reporte dans la seconde condition : $3 + 7k \equiv 5 [11]$, soit $7k \equiv 2 [11]$.

On est ramené à une congruence linéaire en k : c'est exactement le type d'équation que l'inverse modulaire résout d'un coup.

$\text{PGCD}(7; 11) = 1$, donc 7 est inversible modulo 11. Cherchons son inverse.

On teste les multiples de 7 : $7 \times 8 = 56 = 55 + 1$, donc $7 \times 8 \equiv 1 [11]$. L'inverse de 7 modulo 11 est 8.

On multiplie la congruence par 8 : $8 \times 7k \equiv 8 \times 2 [11]$, soit $56k \equiv 16 [11]$.

Comme $56 \equiv 1$ et $16 \equiv 5 [11]$, il vient $k \equiv 5 [11]$.

Il existe donc un entier m tel que $k = 5 + 11m$.

En reportant dans $x = 3 + 7k$: $x = 3 + 7(5 + 11m) = 3 + 35 + 77m = 38 + 77m$.

L'ensemble des solutions est donc $x \equiv 38 [77]$, avec $77 = 7 \times 11$.

Vérification : $38 = 7 \times 5 + 3$, donc $38 \equiv 3 [7]$ ✓ ; et $38 = 11 \times 3 + 5$, donc $38 \equiv 5 [11]$ ✓.

Comparaison avec le chapitre précédent : le balayage aurait exigé de tester jusqu'à 77 valeurs. L'inverse modulaire donne le résultat en trois lignes, et la méthode reste praticable avec des modules à plusieurs chiffres.

Réponse. $x = 3 + 7k$ puis $7k \equiv 2 [11]$ · l'inverse de 7 modulo 11 est 8, d'où $k \equiv 5 [11]$ · $x = 38 + 77m$, soit $x \equiv 38 [77]$.

Rappel de cours. Méthode générale : exprimer x à partir de la première congruence, reporter dans la seconde, résoudre en multipliant par l'inverse modulaire, puis revenir à x . Le module final est le produit des deux modules (premiers entre eux).

Erreur fréquente. Multiplier par un « inverse » sans vérifier qu'il en est un. Un contrôle d'une ligne ($7 \times 8 = 56 \equiv 1$) évite de propager une erreur dans tout le calcul.

Correction de l'exercice 15 - Fractions irréductibles et simplification

Soit d un diviseur commun de $n+1$ et $2n+3$. On multiplie la première expression par 2 : $2(n+1) = 2n+2$.

d divise $2n + 3$ et $2n + 2$, donc leur différence : $(2n + 3) - (2n + 2) = 1$.

Donc $d \mid 1$, c'est-à-dire $d = 1$: la fraction $\frac{n+1}{2n+3}$ est irréductible pour tout n .

Deuxième fraction : soit d un diviseur commun de $3n + 4$ et $n + 1$. On multiplie la seconde par 3 : $3(n + 1) = 3n + 3$.

d divise $(3n + 4) - (3n + 3) = 1$, donc $d = 1$: cette fraction est également toujours irréductible.

Contrôle : $n = 5$ donne $\frac{19}{6}$, irréductible ✓ ; $n = 10$ donne $\frac{34}{11}$, irréductible ✓.

Troisième fraction : soit d un diviseur commun de $2n + 3$ et $5n + 2$.

On élimine n : $5(2n + 3) = 10n + 15$ et $2(5n + 2) = 10n + 4$.

d divise la différence : $(10n + 15) - (10n + 4) = 11$. Donc $d \mid 11$, et comme 11 est premier, d vaut 1 ou 11.

La fraction est réductible exactement quand $d = 11$, c'est-à-dire quand 11 divise $2n + 3$.

On résout $2n + 3 \equiv 0 \pmod{11}$, soit $2n \equiv -3 \equiv 8 \pmod{11}$.

L'inverse de 2 modulo 11 est 6 (car $12 \equiv 1$). En multipliant : $n \equiv 6 \times 8 = 48 \equiv 4 \pmod{11}$.

La fraction est donc réductible si et seulement si $n \equiv 4 \pmod{11}$.

Contrôle : $n = 4$ donne $\frac{11}{22} = \frac{1}{2}$, effectivement réductible ✓. Et $n = 15$ donne $\frac{33}{77} = \frac{3}{7}$, réductible par 11 ✓.

Contre-contrôle : $n = 5$ donne $\frac{13}{27}$, irréductible ✓, et $5 \not\equiv 4 \pmod{11}$ ✓.

Réponse. $\frac{n+1}{2n+3}$ et $\frac{3n+4}{n+1}$ sont irréductibles pour tout n (la combinaison vaut 1) · $\frac{2n+3}{5n+2}$ est réductible si et seulement si $n \equiv 4 \pmod{11}$, et se simplifie alors par 11.

Rappel de cours. Combinaison égale à 1 : irréductible pour tout n . Combinaison égale à un nombre premier p : réductible exactement pour une classe de congruence modulo p , à déterminer.

Erreur fréquente. Conclure « réductible » dès que la combinaison n'est pas 1. Il faut encore trouver POUR QUELS n le diviseur est effectivement atteint.

Correction de l'exercice 16 - Multiples communs et cycles

Les instants d'éclat sont les multiples de 15 pour le premier phare et de 18 pour le deuxième.

Ils coïncident aux multiples communs : la première coïncidence après $t = 0$ est le PPCM.

$15 = 3 \times 5$ et $18 = 2 \times 3^2$, donc $\text{PGCD}(15; 18) = 3$.

$\text{PPCM}(15; 18) = \frac{15 \times 18}{3} = 90$: les deux premiers phares sont synchrones toutes les 90 secondes.

Pour les trois phares, on cherche le PPCM des trois nombres. On passe par la décomposition, plus sûre qu'un calcul en cascade.

$15 = 3 \times 5$, $18 = 2 \times 3^2$, $24 = 2^3 \times 3$.

Le PPCM prend chaque facteur premier au plus grand exposant :

$2^3 \times 3^2 \times 5 = 8 \times 9 \times 5 = 360$.

Les trois phares seront donc synchrones toutes les 360 secondes, soit toutes les 6 minutes.

Contrôle : $360 = 15 \times 24$ ✓, $360 = 18 \times 20$ ✓, $360 = 24 \times 15$ ✓ : c'est bien un multiple commun.

Contrôle de minimalité : 180 est multiple de 15 et de 18, mais $180 = 24 \times 7,5$ n'est pas multiple de 24 ✓.

Troisième question : une heure vaut 3600 secondes.

Les instants de synchronisation sont les multiples de 360 : 360, 720, ..., 3600.

Leur nombre est $\frac{3600}{360} = 10$.

Les trois phares seront donc synchrones 10 fois au cours de l'heure, la dernière fois exactement à $t = 3600$ s.

Réponse. Les deux premiers phares : toutes les 90 secondes · les trois : toutes les 360 secondes, soit 6 minutes · au cours d'une heure : 10 fois.

Rappel de cours. PPCM de plusieurs nombres : décomposer en facteurs premiers et prendre chaque facteur au plus GRAND exposant. La relation $\text{PGCD} \times \text{PPCM} = ab$ ne vaut que pour DEUX nombres.

Erreur fréquente. Appliquer $\text{PGCD} \times \text{PPCM} = abc$ à trois nombres. C'est faux : ici $\text{PGCD}(15; 18; 24) = 3$ et $3 \times 360 = 1080 \neq 15 \times 18 \times 24$.

Correction de l'exercice 17 - Solutions positives d'une équation diophantienne

Algorithme d'Euclide : $23 = 1 \times 17 + 6$; $17 = 2 \times 6 + 5$; $6 = 1 \times 5 + 1$; $5 = 5 \times 1 + 0$.

Le dernier reste non nul est 1 : $\text{PGCD}(23; 17) = 1$, et comme 1 divise 1000, l'équation a des solutions.

Remontée. On part de $1 = 6 - 5$.

On remplace 5 par $17 - 2 \times 6$: $1 = 6 - (17 - 2 \times 6) = 3 \times 6 - 17$.

On remplace 6 par $23 - 17$: $1 = 3(23 - 17) - 17 = 3 \times 23 - 4 \times 17$.

Donc $u = 3$ et $v = -4$. Vérification : $69 - 68 = 1$ ✓.

Solution particulière de l'équation : on multiplie par 1000, ce qui donne $23 \times 3000 + 17 \times (-4000) = 1000$.

Le couple $(3000; -4000)$ est solution — inutilisable tel quel, mais parfait comme point de départ.

Cas général : en soustrayant, $23(x - 3000) + 17(y + 4000) = 0$, soit $23(x - 3000) = -17(y + 4000)$.

17 divise $23(x - 3000)$ et $\text{PGCD}(17; 23) = 1$, donc par Gauss $17 \mid x - 3000$: $x = 3000 - 17k$ (on choisit ce signe pour la suite).

En reportant : $23 \times (-17k) = -17(y + 4000)$, donc $y + 4000 = 23k$ et $y = -4000 + 23k$.

Les solutions entières sont donc $\{(3000 - 17k; -4000 + 23k), k \in \mathbb{Z}\}$.

Contraintes. $x \geq 0$ donne $17k \leq 3000$, soit $k \leq 176,47$, donc $k \leq 176$.

$y \geq 0$ donne $23k \geq 4000$, soit $k \geq 173,91$, donc $k \geq 174$.

Les entiers convenables sont donc $k = 174, 175$ et 176 : il y a exactement TROIS solutions.

$k = 174$: $x = 3000 - 2958 = 42$ et $y = -4000 + 4002 = 2$. Contrôle : $23 \times 42 + 17 \times 2 = 966 + 34 = 1000$ ✓.

$k = 175$: $x = 25$ et $y = 25$. Contrôle : $575 + 425 = 1000$ ✓.

$k = 176 : x = 8$ et $y = 48$. Contrôle : $184 + 816 = 1000$ ✓.

Réponse. $3 \times 23 - 4 \times 17 = 1$ · solutions générales : $x = 3000 - 17k$, $y = -4000 + 23k$ · en entiers naturels : $(42; 2)$, $(25; 25)$ et $(8; 48)$.

Rappel de cours. Le filtrage par les contraintes donne un ENCADREMENT du paramètre. Le nombre de solutions positives est le nombre d'entiers dans cet intervalle — souvent très petit, parfois nul.

Erreur fréquente. Arrondir dans le mauvais sens. $k \leq 176,47$ donne $k \leq 176$, mais $k \geq 173,91$ donne $k \geq 174$: les deux arrondis vont dans des directions opposées.

Correction de l'exercice 18 - Résoudre une congruence avec un grand module

On calcule PGCD(17; 26) : $26 = 1 \times 17 + 9$; $17 = 1 \times 9 + 8$; $9 = 1 \times 8 + 1$; $8 = 8 \times 1 + 0$.

Le PGCD vaut 1 : 17 et 26 sont premiers entre eux, donc 17 est inversible modulo 26.

Une équation $ax \equiv b [n]$ avec a inversible admet exactement UNE solution modulo n : on multiplie simplement par l'inverse.

Remontée pour l'inverse. On part de $1 = 9 - 8$.

On remplace 8 par $17 - 9$: $1 = 9 - (17 - 9) = 2 \times 9 - 17$.

On remplace 9 par $26 - 17$: $1 = 2(26 - 17) - 17 = 2 \times 26 - 3 \times 17$.

Donc $-3 \times 17 + 2 \times 26 = 1$. En réduisant modulo 26 : $-3 \times 17 \equiv 1 [26]$.

L'inverse de 17 est donc -3 , soit $-3 + 26 = 23$ entre 0 et 25.

Vérification : $17 \times 23 = 391$. Or $391 = 26 \times 15 + 1 = 390 + 1$, donc $17 \times 23 \equiv 1 [26]$ ✓.

Résolution : on multiplie les deux membres de $17x \equiv 5 [26]$ par 23.

$23 \times 17x \equiv 23 \times 5 [26]$, soit $x \equiv 115 [26]$ puisque $23 \times 17 \equiv 1$.

On réduit : $115 = 26 \times 4 + 11$, donc $x \equiv 11 [26]$.

Vérification directe : $17 \times 11 = 187$, et $187 = 26 \times 7 + 5 = 182 + 5$, donc $17 \times 11 \equiv 5 [26]$ ✓.

L'ensemble des solutions est $\{11 + 26k, k \in \mathbb{Z}\}$ — une seule classe, comme annoncé.

Réponse. PGCD(17; 26) = 1, donc une unique solution modulo 26 · $-3 \times 17 + 2 \times 26 = 1$, l'inverse de 17 est 23 · $x \equiv 23 \times 5 = 115 \equiv 11 [26]$.

Rappel de cours. $ax \equiv b [n]$ avec PGCD($a; n$) = 1 : la solution est $x \equiv a'b [n]$, où a' est l'inverse de a . Unique modulo n , toujours.

Erreur fréquente. Oublier de réduire l'inverse entre 0 et $n - 1$. -3 est correct, mais 23 est la forme attendue dans une réponse.

Correction de l'exercice 19 - Problème type bac : congruences et dénombrement

La première condition s'écrit $n = 1 + 5k$. On reporte dans la seconde : $1 + 5k \equiv 3 [8]$, soit $5k \equiv 2 [8]$.

PGCD(5; 8) = 1, donc 5 est inversible modulo 8. On cherche son inverse : $5 \times 5 = 25 = 24 + 1 \equiv 1 [8]$, donc l'inverse de 5 est 5.

On multiplie par 5 : $25k \equiv 10 [8]$, soit $k \equiv 2 [8]$.

Pour $k = 2$: $n = 1 + 10 = 11$. C'est une solution particulière.

Vérification : $11 = 5 \times 2 + 1$ ✓ et $11 = 8 + 3$ ✓.

Cas général : $k \equiv 2 \pmod{8}$ signifie $k = 2 + 8m$, donc $n = 1 + 5(2 + 8m) = 11 + 40m$.

On peut aussi raisonner directement : si n est solution, alors $n - 11$ est divisible par 5 (car $n \equiv 11 \equiv 1 \pmod{5}$) et par 8 (car $n \equiv 11 \equiv 3 \pmod{8}$).

Comme 5 et 8 sont premiers entre eux, leur produit 40 divise $n - 11$ — c'est le corollaire du théorème de Gauss.

Réciproquement, tout $n \equiv 11 \pmod{40}$ vérifie les deux conditions. L'ensemble des solutions est donc exactement $n \equiv 11 \pmod{40}$.

Troisième question : les solutions entre 1 et 1000 sont les $n = 11 + 40m$ avec $1 \leq 11 + 40m \leq 1000$.

La borne inférieure donne $40m \geq -10$, donc $m \geq 0$ (pour n entier naturel non nul).

La borne supérieure donne $40m \leq 989$, soit $m \leq 24,725$, donc $m \leq 24$.

Les valeurs possibles de m sont donc $0, 1, \dots, 24$: il y a 25 solutions.

La plus grande correspond à $m = 24$: $n = 11 + 960 = 971$.

Contrôle : $971 = 5 \times 194 + 1$ ✓ et $971 = 8 \times 121 + 3$ ✓. Et la suivante, 1011, dépasse bien 1000 ✓.

Réponse. Solution particulière : 11 · l'ensemble des solutions est $n \equiv 11 \pmod{40}$ · il y a 25 solutions entre 1 et 1000, la plus grande étant 971.

Rappel de cours. Corollaire de Gauss : si b et c sont premiers entre eux et divisent tous deux N , alors $bc \mid N$. C'est lui qui justifie le passage au module $40 = 5 \times 8$.

Erreur fréquente. Prendre PPCM(5 ; 8) = 40 sans justifier. Ici les modules sont premiers entre eux, donc le PPCM est bien le produit — ce ne serait pas le cas avec 4 et 6.

Correction de l'exercice 20 - Problème de synthèse : Bézout et déchiffrement

Algorithme d'Euclide : $26 = 2 \times 11 + 4$; $11 = 2 \times 4 + 3$; $4 = 1 \times 3 + 1$; $3 = 3 \times 1 + 0$.

Le PGCD vaut 1, qui divise 1 : (E) admet des solutions.

Remontée : $1 = 4 - 3$.

On remplace 3 par $11 - 2 \times 4$: $1 = 4 - (11 - 2 \times 4) = 3 \times 4 - 11$.

On remplace 4 par $26 - 2 \times 11$: $1 = 3(26 - 2 \times 11) - 11 = 3 \times 26 - 7 \times 11$.

Donc $-7 \times 11 + 3 \times 26 = 1$, qu'on réécrit sous la forme de (E) : $11 \times (-7) - 26 \times (-3) = 1$.

Le couple $(-7 ; -3)$ est solution. Vérification : $-77 + 78 = 1$ ✓.

Cas général : soit $(x ; y)$ solution. En soustrayant : $11(x + 7) - 26(y + 3) = 0$, soit $11(x + 7) = 26(y + 3)$.

26 divise $11(x + 7)$, et PGCD(26 ; 11) = 1, donc par Gauss $26 \mid x + 7$: $x = -7 + 26k$.

En reportant : $11 \times 26k = 26(y + 3)$, donc $y = -3 + 11k$.

Les solutions de (E) sont $\{(-7 + 26k ; -3 + 11k), k \in \mathbb{Z}\}$.

Inverse de 11 modulo 26 : de $11 \times (-7) - 26 \times (-3) = 1$, on tire $11 \times (-7) \equiv 1 \pmod{26}$.

L'inverse est donc $-7 \equiv 19 \pmod{26}$. Vérification : $11 \times 19 = 209 = 26 \times 8 + 1 = 208 + 1$ ✓.

Résolution de $11x \equiv 7 \pmod{26}$: on multiplie par 19, ce qui donne $x \equiv 19 \times 7 = 133 \pmod{26}$.

On réduit : $133 = 26 \times 5 + 3$, donc $x \equiv 3 \pmod{26}$.

Vérification : $11 \times 3 = 33 = 26 + 7$, donc $11 \times 3 \equiv 7 \pmod{26}$ ✓.

Déchiffrement du code. On part de $y \equiv 11x + 4 \pmod{26}$, donc $y - 4 \equiv 11x \pmod{26}$.

On multiplie par l'inverse 19 : $19(y - 4) \equiv 19 \times 11x \equiv x \pmod{26}$.

La formule de déchiffrement est donc $x \equiv 19(y - 4) \pmod{26}$.

Décodons G , de rang $y = 6$: $x \equiv 19 \times (6 - 4) = 19 \times 2 = 38 \pmod{26}$, et $38 = 26 + 12$, donc $x \equiv 12$.

Le rang 12 correspond à la lettre M . La lettre G décode donc en M .

Contrôle dans l'autre sens : $11 \times 12 + 4 = 136$, et $136 = 26 \times 5 + 6$, donc M se code bien en rang 6, c'est-à-dire G ✓.

Réponse. (E) : $\text{PGCD}(11; 26) = 1$, solution particulière $(-7; -3)$, solutions $x = -7 + 26k$, $y = -3 + 11k$ · inverse de 11 modulo 26 : $19 \cdot 11x \equiv 7 \pmod{26} \Rightarrow x \equiv 3 \pmod{26}$ · déchiffrement : $x \equiv 19(y - 4) \pmod{26}$, et G décode en M .

Rappel de cours. Chaîne complète du chapitre : Euclide donne le PGCD, la remontée donne Bézout, Bézout donne l'inverse modulaire, l'inverse donne le déchiffrement. Chaque maillon se vérifie en une ligne.

Erreur fréquente. Confondre les deux inverses en jeu. Ici 19 est l'inverse de 11 modulo 26 ; le -7 de Bézout est le même nombre, simplement écrit sous une autre forme.