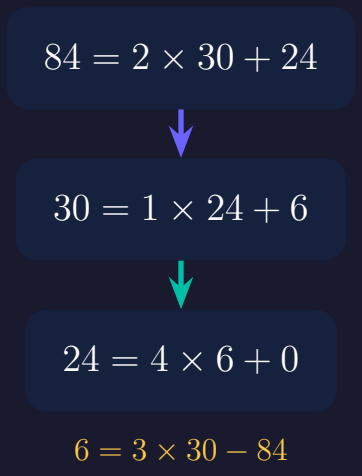
FICHE 05

PGCD, Bézout et Gauss

Euclide ▪ Identité de Bézout ▪ Équations entières



Terminale — Option Mathématiques expertes — Programme officiel

Cours | 15 exercices | Problème guidé | Corrigés

Table des matières

1 Pourquoi ce chapitre ?

1.1 Le problème fondamental : quels nombres peut-on fabriquer ?

Avec des combinaisons entières de 6 et 10, tu peux fabriquer $4 = 10 - 6$ et $2 = 2 \times 6 - 10$, mais jamais 3 : chaque combinaison est paire. Le PGCD va préciser cette obstruction. Bézout montrera ensuite qu'elle est la seule obstruction pour une équation $ax + by = c$ dans les entiers.

Intuition | Calculer et construire sont deux tâches liées

Euclide répond « quel est le PGCD ? ». En remontant les mêmes divisions, Bézout répond « comment le fabriquer avec les nombres de départ ? ». Nous allons conserver les traces du calcul : elles deviendront une méthode de résolution.

Prérequis. Divisibilité, combinaison linéaire entière, division euclidienne et congruences de la fiche 4. Pour les divisions de l'algorithme, les restes sont positifs ou nuls.

Méthode | Objectifs

Calculer un PGCD ; remonter Euclide ; démontrer Bézout et Gauss ; inverser modulo n ; résoudre $ax + by = c$ et $ax \equiv b \pmod{n}$; reconnaître les paramètres entiers libres.

Ces notions appartiennent au socle. Le PPCM et le théorème chinois final sont des prolongements construits à partir de Bézout et Gauss.

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 Pourquoi remplacer une paire par une autre ?

Les diviseurs communs de 84 et 30 divisent aussi $84 - 2 \times 30 = 24$. Inversement, ceux de 30 et 24 divisent $2 \times 30 + 24 = 84$. Les paires $(84, 30)$ et $(30, 24)$ ont donc exactement les mêmes diviseurs communs. La seconde paire est plus petite : on a progressé sans perdre l'information cherchée.

2.2 Le calcul peut se lire dans les deux sens

Les divisions suivantes conduisent à $30 = 24 + 6$, puis $24 = 4 \times 6$. Le PGCD est 6. Relis maintenant à l'envers : $6 = 30 - 24 = 30 - (84 - 2 \times 30) = 3 \times 30 - 84$. Cette égalité indique les coefficients qui fabriquent le PGCD. Les signes négatifs sont autorisés, puisque l'on travaille dans $\mathbb{Z}$.

2.3 Une solution n'est pas toutes les solutions

Si $3x+5y=1$, le couple $(2,-1)$ convient. En ajoutant 5 à x et en retirant 3 à y, la somme reste inchangée : on ajoute 15 puis on enlève 15. Le paramètre entier décrira ces déplacements. Gauss permettra de prouver qu'ils couvrent toutes les solutions, et pas seulement une famille commode.

Attention | Une contrainte supplémentaire change la réponse

Les coefficients d'une identité de Bézout peuvent être négatifs. Dans un problème de quantités physiques, on imposera ensuite $x, y \geq 0$. Il faut d'abord résoudre dans les entiers, puis sélectionner les paramètres compatibles avec la situation.

3 Le cours formel

3.1 PGCD et entiers premiers entre eux

Définition | PGCD

Pour deux entiers a, b non tous deux nuls, le PGCD est le plus grand de leurs diviseurs communs positifs. On le note $\gcd(a,b)$. Il est positif et ne dépend pas des signes : $\gcd(a,b)=\gcd(|a|,|b|)$. Pour $a \neq 0$, $\gcd(a,0)=|a|$. On adopte aussi la convention $\gcd(0,0)=0$.

Deux entiers sont **premiers entre eux** lorsque leur PGCD vaut 1. Cela ne signifie pas qu'ils sont chacun premiers : 8 et 15 sont premiers entre eux bien que chacun soit composé.

Exemple | Lister sur un petit cas

Les paires $1\times 18, 2\times 9, 3\times 6$ donnent les diviseurs positifs de 18 : $1,2,3,6,9,18$. Pour 30, les paires $1\times 30, 2\times 15, 3\times 10, 5\times 6$ donnent $1,2,3,5,6,10,15,30$. En comparant, les nombres présents dans les deux listes sont $1,2,3,6$. Le plus grand est 6 : le PGCD vaut 6. Cela ne signifie pas que 6 est leur seul diviseur commun ; c'est le plus grand diviseur *positif* commun. Les signes négatifs n'ajoutent pas de diviseur positif nouveau.

À toi d'essayer : Premiers entre eux ne veut pas dire premiers

8 et 9 sont-ils premiers entre eux ? Et 8 et 12 ? Donne un diviseur commun maximal dans chaque cas.

Pour démarrer. Compare les diviseurs positifs, et non le fait que chaque nombre soit premier ou composé.

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

Indices, p. 26 Explication, p. 29

3.2 Algorithme d'Euclide et invariant des diviseurs

Théorème | Étape fondamentale

Si $a = bq + r$ avec $b > 0$ et $0 \leq r < b$, alors a, b et b, r ont exactement les mêmes diviseurs communs. En particulier, $\gcd(a,b)=\gcd(b,r)$.

Démonstration | Les deux implications

Nous voulons montrer que les listes de diviseurs communs sont identiques. Cela demande deux sens. Si $d \mid a$ et $d \mid b$, écrivons $a = du, b = dv$ avec u, v entiers. Comme $r = a - bq$, $r = du - dvq = d(u - vq)$, donc $d \mid r$. Ce diviseur divise alors b et r.
Réciproquement, si $d \mid b$ et $d \mid r$, écrivons $b = ds, r = dt$. Alors $a = bq + r = dsq + dt = d(sq + t)$, donc $d \mid a$. Il divise donc aussi a et b. Les deux listes de diviseurs communs sont les mêmes ; leur plus grand élément positif, le PGCD, est donc le même. La division change les nombres, mais conserve exactement l'information recherchée.

Méthode | Calculer jusqu'au reste nul

Remplace d'abord a, b par leurs valeurs absolues. Divise le plus grand par le plus petit, puis le diviseur par le reste. Continue jusqu'au premier reste nul. Le dernier reste non nul est le PGCD.

La procédure s'arrête : les restes non nuls forment une suite strictement décroissante d'entiers naturels. À la dernière étape, le PGCD de $(r, 0)$ vaut r ; l'invariance prouve que c'est le PGCD initial.

Exemple | Un calcul complet

Partons du couple $(252, 198)$. La division $252 = 1 \times 198 + 54$ permet de remplacer ce couple par $(198, 54)$ sans changer ses diviseurs communs. Puis $198 = 3 \times 54 + 36$ donne $(54, 36)$; $54 = 1 \times 36 + 18$ donne $(36, 18)$; enfin $36 = 2 \times 18 + 0$ donne $(18, 0)$.
Tous les diviseurs de 18 divisent aussi zéro. Le PGCD final vaut donc 18, et l'invariance à chaque étape prouve $\gcd(252, 198) = 18$. Les restes étaient $54, 36, 18, 0$: nous gardons le dernier *non nul*. Le quotient final 2 a un autre rôle, et n'est pas le PGCD.

À toi d'essayer : Lire la dernière ligne

Calcule le PGCD de 84 et 30.
Pour démarrer. À chaque étape, le diviseur et le reste deviennent le nouveau couple.

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

Indices, p. 26 Explication, p. 29

3.3 Remonter Euclide et démontrer Bézout

Théorème | Identité de Bézout

Pour a, b non tous deux nuls, il existe $u, v \in \mathbb{Z}$ tels que $au+bv = d$, où $d = \gcd(a, b)$. En particulier,

$$\gcd(a, b) = 1 \iff \exists u, v \in \mathbb{Z},\ au + bv = 1.$$

Démonstration | Existence et caractérisation

Construire la combinaison. Pour des nombres positifs, les deux nombres de départ s'écrivent $a = 1a+0b$ et $b = 0a+1b$. Supposons que deux nombres successifs d'Euclide s'écrivent $r = au+bv$ et $s = au' + bv'$. Le reste suivant est $r - qs$, donc

$$r - qs = a(u - qu') + b(v - qv').$$

Les nouveaux coefficients sont entiers puisque tous les coefficients précédents et le quotient q le sont. Cette propriété est vraie au départ et se conserve à chaque division. Le dernier reste non nul d est donc encore une combinaison $au + bv$: c'est l'identité annoncée.
Si un entier initial est négatif, l'algorithme travaille sur sa valeur absolue ; on change ensuite le signe de son coefficient pour réécrire l'identité avec l'entier initial. Si l'un est nul, par exemple $b = 0, a \neq 0$, $d = |a|$ s'écrit a ou $-a$ selon son signe.
Caractériser le PGCD 1. Si le PGCD vaut 1, l'identité construite fournit $au+bv = 1$. Inversement, supposons une telle identité connue. Tout diviseur commun positif h divise a et b, donc la combinaison $au+bv = 1$. Le seul diviseur positif de 1 est 1 ; ainsi tous les diviseurs communs positifs se réduisent à 1, et le PGCD vaut 1. Nous avons prouvé les deux directions.

Exemple | Remontée détaillée

Le dernier reste non nul est $18 = 54 - 36$. Nous voulons éliminer 36, puis 54, pour ne garder que 252 et 198. La division précédente donne $36 = 198 - 3 \times 54$. Donc

$$18 = 54 - (198 - 3 \times 54) = 54 - 198 + 3 \times 54 = 4 \times 54 - 198.$$

Le signe moins devant la parenthèse change le signe de ses deux termes. La première division donne $54 = 252 - 198$. En remplaçant,

$$18 = 4(252 - 198) - 198 = 4 \times 252 - 4 \times 198 - 198 = 4 \times 252 - 5 \times 198.$$

Ainsi $u = 4, v = -5$. Vérification numérique : $4 \times 252 = 1008$ et $5 \times 198 = 990$, donc leur différence est bien 18. Cette remontée produit une identité exacte, pas seulement la valeur du PGCD.

Propriété | Tous les diviseurs communs

Les diviseurs communs de a, b sont exactement les diviseurs de leur PGCD. De plus, si $d = \gcd(a, b)$, alors a/d et b/d sont premiers entre eux.

Démonstration | Conséquences de Bézout

Notons $d = \gcd(a, b) > 0$ et choisissons u, v tels que $au + bv = d$. Si h divise a et b, il divise toute combinaison entière, donc il divise d. Réciproquement, d divise a et b par définition ; si h divise d, la transitivité montre que h divise aussi a et b. Les diviseurs de d sont donc exactement les diviseurs communs.
Divisons maintenant l'identité de Bézout par d, non nul : $(a/d)u + (b/d)v = 1$. Les nombres a/d et b/d sont entiers parce que d les divise. Ils possèdent une combinaison entière égale à 1 ; la caractérisation de Bézout prouve donc qu'ils sont premiers entre eux. Il ne s'agit pas simplement de dire qu'ils sont « plus petits » : c'est l'identité égale à 1 qui justifie leur coprimalité.

À toi d'essayer : Fabriquer le 1 qui permet de simplifier

À partir de $17 = 2 \times 7 + 3$ et $7 = 2 \times 3 + 1$, écris 1 comme combinaison de 17 et 7.
Pour démarrer. Isole 1 dans la dernière division, puis remplace 3 avec la première.

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

Indices, p. 26 Explication, p. 29

3.4 Le théorème de Gauss

Théorème | Simplifier une divisibilité

Si $a \mid bc$ et $\gcd(a, b) = 1$, alors $a \mid c$.

Démonstration | Preuve à partir de Bézout

Nous savons $a \mid bc$ et $\gcd(a, b) = 1$. Cette seconde hypothèse permet d'écrire $au + bv = 1$ avec u, v entiers. Pourquoi chercher 1 ? Parce que multiplier cette identité par c va faire apparaître c seul d'un côté : $auc + bvc = c$.
Le terme $auc = a(uc)$ est un multiple de a. Pour le second, l'hypothèse de divisibilité donne $bc = ak$ avec $k \in \mathbb{Z}$, donc $bvc = v(bc) = a(vk)$. Les deux termes sont bien multiples de a ; leur somme s'écrit explicitement $c = a(uc + vk)$. La parenthèse est entière, donc $a \mid c$. C'est la coprimalité avec b, et non le seul fait que a divise le produit, qui permet de supprimer ce facteur.

Attention | Une hypothèse indispensable

$6 \mid 2 \times 3$ mais $6 \nmid 3$. On ne peut pas retirer le facteur 2 car $\gcd(6, 2) = 2 \neq 1$. Le rôle du PGCD n'est pas une formalité : il empêche de répartir les facteurs de a entre les deux termes du produit.

Propriété | Combiner deux divisibilités

Si $a, b > 0$ sont premiers entre eux et divisent tous deux n, alors $ab \mid n$.

Démonstration | Utilisation de Gauss

Comme $a \mid n$, il existe $k \in \mathbb{Z}$ tel que $n = ak$. Nous savons aussi $b \mid n$, donc $b \mid ak$. Les entiers b et a sont premiers entre eux ; Gauss, avec diviseur b, facteur supprimé a et facteur restant k, donne $b \mid k$. Il existe donc $\ell \in \mathbb{Z}$ tel que $k = b\ell$. En remplaçant, $n = a(b\ell) = ab\ell$, donc $ab \mid n$.
La coprimalité a été utilisée au passage de $b \mid ak$ à $b \mid k$. Sans elle, ce passage est faux : 4 et 6 divisent 12, mais $4 \times 6 = 24$ ne divise pas 12. On ne peut pas additionner les facteurs communs deux fois.

Une preuve à construire : Construire la simplification

Si $7 \mid 3n$, démontre $7 \mid n$ sans utiliser directement le nom du théorème.
Pour démarrer. Multiplie l'égalité $1 = 7 - 2 \times 3$ par n, puis utilise l'hypothèse.

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

Indices, p. 26 Explication, p. 29

À toi d'essayer : Vérifier avant de supprimer un facteur

Si $15 \mid 4n$, que peux-tu conclure ? Pourquoi le même raisonnement ne donne-t-il pas $15 \mid n$ à partir de $15 \mid 5n$?
Pour démarrer. Vérifie le PGCD avant d'invoquer Gauss et cherche un contre-exemple lorsque l'hypothèse échoue.

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

Indices, p. 27 Explication, p. 30

3.5 Inverses et congruences linéaires

Théorème | Quand un inverse existe-t-il ?

Pour $n \geq 2$, l'entier a possède un inverse modulo n si et seulement si $\gcd(a, n) = 1$. Un coefficient u de l'identité $au + nv = 1$ fournit l'inverse. Cet inverse est unique modulo n.

Démonstration | Existence et unicité

Nécessité. Si u est un inverse de a modulo n, $au \equiv 1$ signifie $au - 1 = nk$ pour un entier k. Réarrangeons : $au + n(-k) = 1$. C'est une identité de Bézout pour a, n, donc $\gcd(a, n) = 1$.
Suffisance. Si $\gcd(a, n) = 1$, Bézout fournit $au + nv = 1$. Modulo n, le terme nv disparaît car c'est un multiple de n ; il reste $au \equiv 1$. Le coefficient u est donc un inverse.
Unicité modulo n. Si u et v sont deux inverses, $au - 1$ et $av - 1$ sont multiples de n. Leur différence $a(u - v)$ l'est aussi. Comme $\gcd(n, a) = 1$, Gauss donne $n \mid (u - v)$, soit $u \equiv v \pmod{n}$. Les inverses peuvent être des entiers différents, mais ont tous le même reste : par exemple -5 et 38 représentent le même inverse modulo 43.

Exemple | Inverse de 17 modulo 43

Les divisions sont $43 = 2 \times 17 + 9$, $17 = 1 \times 9 + 8$, $9 = 1 \times 8 + 1$. Le reste 1 prouve la coprimalité. Remontons : $1 = 9 - 8 = 9 - (17 - 9) = 2 \times 9 - 17 = 2(43 - 2 \times 17) - 17 = 2 \times 43 - 5 \times 17$. Modulo 43, cela donne $17(-5) \equiv 1$. L'inverse est donc -5, ou $-5 + 43 = 38$. Multiplions $17x \equiv 7$ par -5 : $x \equiv -35 \equiv 8 \pmod{43}$. La famille est $x = 8 + 43k$. Contrôle sur le représentant : $17 \times 8 = 136 = 3 \times 43 + 7$. Ajouter 43 à x ajoute un multiple de 43 au produit, donc toute la famille convient.

Théorème | Cas général $ax \equiv b \pmod{n}$

Soit $d = \gcd(a, n)$. Il existe des solutions si et seulement si $d \mid b$. Lorsque c'est le cas, divise a, b, n par d : l'équation équivaut à

$$(a/d)x \equiv b/d \pmod{n/d}.$$

Le nouveau coefficient et le nouveau module sont premiers entre eux. Une classe modulo n/d donne exactement d classes modulo n.

Démonstration | Pourquoi le module change

La congruence $ax \equiv b \pmod{n}$ signifie qu'il existe un entier y tel que $ax - ny = b$. Posons $d = \gcd(a, n)$. Puisque d divise a et n, il divise le membre gauche pour tous entiers x, y. Donc $d \mid b$ est nécessaire ; si cette condition échoue, nous arrêtons : aucune solution.
Si $d \mid b$, écrivons $a = da'$, $n = dn'$ et $b = db'$. L'égalité devient $d(a'x - n'y) = db'$. Comme $d > 0$, elle équivaut à $a'x - n'y = b'$, donc à $a'x \equiv b' \pmod{n'}$. Le module est bien devenu n/d, car le coefficient de l'entier libre y a aussi été divisé.
Les nombres a', n' sont premiers entre eux. Si $n' \geq 2$, un inverse fournit une classe $x = x_0 + n'k$. Si $n' = 1$, tous les entiers conviennent. Dans le premier cas, prenons $k = 0, \ldots, d-1$: les valeurs obtenues représentent d classes distinctes modulo $dn' = n$. En effet, deux valeurs diffèrent de $n'(k - \ell)$, multiple de n seulement si $d \mid (k - \ell)$; dans cette liste cela impose $k = \ell$. Les autres k répètent ces classes.

Pour $6x \equiv 9 \pmod{15}$, le PGCD des deux coefficients 6 et 15 vaut 3, et il divise 9. Diviser l'égalité entière $6x - 15k = 9$ par 3 donne $2x - 5k = 3$, soit $2x \equiv 3 \pmod{5}$. L'inverse de 2 modulo 5 est 3, car $2 \times 3 = 6 \equiv 1$. Multiplier par 3 donne $x \equiv 9 \equiv 4 \pmod{5}$, donc $x = 4 + 5t$. Dans l'intervalle $0 \leq x < 15$, les valeurs de t sont 0,1,2 : les restes sont $4, 9, 14$. Les produits par 6 valent 24,54,84, tous de reste 9 modulo 15.

À toi d'essayer : Utiliser le bon coefficient de Bézout

Utilise $1 = 5 \times 7 - 2 \times 17$ pour résoudre $7x \equiv 3 \pmod{17}$.
Pour démarrer. Réduis l'identité de Bézout modulo 17 pour savoir quel terme disparaît.

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

Indices, p. 27 Explication, p. 30

3.6 Équations diophantiennes : toutes les solutions

Théorème | Équation $ax + by = c$

Pour $a, b \neq 0$, pose $d = \gcd(a, b)$. L'équation a des solutions entières si et seulement si $d \mid c$. Si (x_0, y_0) est une solution particulière, toutes les solutions sont

$$x = x_0 + (b/d)k, \qquad y = y_0 - (a/d)k, \qquad k \in \mathbb{Z}.$$

Démonstration | Nécessité, construction, exhaustivité

1. Tester l'existence. Le PGCD d divise a et b, donc toute combinaison $ax + by$. Si d ne divise pas c, l'équation est impossible. Si $c = dt$, Bézout fournit $au + bv = d$; multiplier par t donne $a(ut) + b(vt) = c$. Le couple $(x_0, y_0) = (ut, vt)$ est une solution particulière.

2. Ne pas confondre un couple avec toutes les solutions. Prenons une solution quelconque (x, y) et soustrayons $ax_0 + by_0 = c$: $a(x - x_0) + b(y - y_0) = 0$. Posons $a' = a/d, b' = b/d$, premiers entre eux. Après division par d, $a'(x - x_0) = -b'(y - y_0)$.
Le membre droit est divisible par b', donc $b' \mid a'(x - x_0)$. Gauss permet de supprimer a' parce que $\gcd(a', b') = 1$: $b' \mid (x - x_0)$. Écrivons $x - x_0 = b'k$ avec $k \in \mathbb{Z}$. En remplaçant, $a'b'k = -b'(y - y_0)$. Comme $b' \neq 0$, on divise par lui : $y - y_0 = -a'k$.
3. Vérifier que toute la famille convient. Pour tout entier k, substituer $x = x_0 + b'k$, $y = y_0 - a'k$ donne $ax + by = ax_0 + by_0 + (ab' - ba')k = c$, car $ab' = ba' = ab/d$. Chaque solution figure donc dans la famille, et chaque membre de la famille est solution. Ces deux sens assurent l'exhaustivité.

Exemple | Contraintes de positivité

Le couple $(2, -1)$ convient puisque $3 \times 2 + 5(-1) = 1$. Les coefficients 3 et 5 sont premiers entre eux. Le théorème donne donc $x = 2 + 5k$, $y = -1 - 3k$, $k \in \mathbb{Z}$.
Imposer $x \geq 0$ donne $k \geq -2/5$. Comme k est entier, cela signifie $k \geq 0$. Imposer $y \geq 0$ donne $-3k \geq 1$, donc $k \leq -1/3$ après division par un nombre négatif ; pour un entier, $k \leq -1$. Aucune valeur ne peut satisfaire les deux bornes. Il existe une infinité de couples entiers, mais aucun dont les deux coordonnées soient positives ou nulles.

Si un coefficient est nul, traite l'équation directement. Par exemple $0x + by = c$ impose $y = c/b$ entier, puis x est libre. Si les deux coefficients sont nuls, tout couple convient pour $c = 0$, aucun sinon.

À toi d'essayer : Passer d'un couple à tous les couples

Résous $3x + 5y = 1$ dans les entiers, puis impose x et y positifs ou nuls.
Pour démarrer. Soustrais le couple particulier, puis impose les deux inégalités sur le même paramètre.

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

Indices, p. 27 Explication, p. 30

3.7 Euclide étendu et PPCM

```python
def bezout(a, b):
    r0, r1 = abs(a), abs(b)
    u0, u1, v0, v1 = 1, 0, 0, 1
    while r1 != 0:
        q = r0 // r1
        r0, r1 = r1, r0 - q*r1
        u0, u1 = u1, u0 - q*u1
        v0, v1 = v1, v0 - q*v1
    return r0, u0*(1 if a >= 0 else -1), v0*(1 if b >= 0 else -1)
```

Au départ, $r_0 = |a| = |a| \times 1 + |b| \times 0$ et $r_1 = |b| = |a| \times 0 + |b| \times 1$. Les deux restes sont donc accompagnés de coefficients qui permettent de les reconstruire à partir des entrées.

Supposons ces deux identités vraies avant un tour. Le nouveau reste est $r_0 - qr_1$. En remplaçant chaque reste par sa combinaison, il devient $|a|(u_0 - qu_1) + |b|(v_0 - qv_1)$. Voilà pourquoi on effectue sur les coefficients exactement la même soustraction que sur les restes. L'ancien reste r_1 et ses coefficients deviennent la première ligne ; le nouveau reste et ses coefficients deviennent la seconde. Python évalue les membres droits avant les affectations, ce qui conserve les anciennes valeurs pendant le calcul.

Les restes positifs diminuent strictement, donc la boucle s'arrête. À l'arrêt, $r_1 = 0$ et $r_0 = d$, le PGCD. On a $d = |a|u_0 + |b|v_0$. Si $a < 0$, remplacer u_0 par $-u_0$ transforme $|a|u_0$ en $a(-u_0)$; on fait de même pour

b. Les signes dans le retour assurent donc $au + bv = d$ pour les entrées signées. Si les deux entrées sont nulles, la boucle est ignorée et le retour respecte la convention $d = 0$.

Propriété | PPCM, prolongement

Pour $a, b > 0$, le plus petit multiple commun positif vaut $\operatorname{ppcm}(a, b) = ab/\operatorname{gcd}(a, b)$.

Posons $d = \operatorname{gcd}(a, b)$, $a = da'$ et $b = db'$. Le cours a prouvé que a', b' sont premiers entre eux. Le nombre $M = da'b'$ est positif ; il vaut ab' et aussi ba', donc est multiple de a et de b.

Prenons maintenant un multiple commun positif m. Comme $a \mid m$, écrivons $m = da'k$. Comme $b \mid m$, il existe aussi ℓ tel que $m = db'\ell$. Diviser l'égalité $da'k = db'\ell$ par $d > 0$ donne $a'k = b'\ell$, donc $b' \mid a'k$. Gauss s'applique puisque $\operatorname{gcd}(a', b') = 1 : b' \mid k$. Écrivons $k = b't$. Alors $m = da'b't = Mt$.

Le nombre t est un entier positif puisque $m, M > 0$, donc $t \geq 1$ et $m \geq M$. Ainsi M est lui-même un multiple commun et aucun multiple commun positif n'est plus petit. Enfin $ab/d = (da')(db')/d = da'b' = M$, ce qui prouve la formule.

À toi d'essayer : PGCD ou PPCM selon la question

Deux événements reviennent tous les 12 et 18 jours et ont lieu ensemble aujourd'hui. Quand se reproduiront-ils ensemble pour la première fois ?
Pour démarrer. Le jour recherché doit être un multiple de chacune des deux périodes.

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

Indices, p. 27 Explication, p. 30

4 Boîte à outils — rendre la solution exhaustive

4.1 Trouver tous les couples et imposer une contrainte

Exemple | Résoudre $14x + 21y = 70$ dans les entiers

Les trois termes sont divisibles par 7, donc l'équation équivaut à $2x+3y = 10$. Un couple particulier est $(5, 0)$, car $2 \times 5 = 10$. Soustraire cette solution donne $2(x - 5) + 3y = 0$, donc $3 \mid 2(x - 5)$. Comme 2 et 3 sont premiers entre eux, $3 \mid (x - 5)$; écrivons $x = 5 + 3k$. Remplacer donne $2(5 + 3k) + 3y = 10$, puis $6k + 3y = 0$, donc $y = -2k$.
Pour tout entier k, $14(5 + 3k) + 21(-2k) = 70 + 42k - 42k = 70$. La famille est donc exacte. Si $x, y \geq 0$, les contraintes sont $k \geq -5/3$ et $k \leq 0$, donc $k = -1$ ou 0. Elles donnent $(2, 2)$ et $(5, 0)$, qui vérifient l'équation initiale.

4.2 Une congruence avec plusieurs classes

Pour $12x \equiv 18 \pmod{30}$, le PGCD vaut 6. Comme 6 divise 18, la réduction donne $2x \equiv 3 \pmod 5$. L'inverse de 2 modulo 5 est 3 : $x \equiv 4 \pmod 5$. Entre 0 et 29, les solutions sont 4,9,14,19,24,29 : six classes, exactement le PGCD initial.

Pour $12x \equiv 17 \pmod{30}$, la condition d'existence échoue puisque 6 ne divise pas 17. Il ne faut pas poursuivre une recherche d'inverse qui ne peut pas résoudre cette équation.

4.3 Une méthode pour inverser de grands coefficients

Exemple | Inverse de 23 modulo 41

Euclide donne $41 = 23 + 18$, $23 = 18 + 5$, $18 = 3 \times 5 + 3$, $5 = 3 + 2$, $3 = 2 + 1$. Remontons en gardant les parenthèses :

$$\begin{aligned} 1 &= 3 - 2 = 3 - (5 - 3) = 2 \times 3 - 5 \\ &= 2(18 - 3 \times 5) - 5 = 2 \times 18 - 7 \times 5 \\ &= 2 \times 18 - 7(23 - 18) = 9 \times 18 - 7 \times 23 \\ &= 9(41 - 23) - 7 \times 23 = 9 \times 41 - 16 \times 23. \end{aligned}$$

Le coefficient de 23 est -16 : c'est son inverse modulo 41. Le représentant positif est $-16+41 = 25$. Vérification : $23\times25 = 575 = 14\times41+1$. Le coefficient 9 concerne 41 et disparaît dans la réduction modulo 41.

4.4 PGCD d'une famille : ne pas s'arrêter aux possibilités

Une combinaison peut montrer qu'un PGCD divise une constante sans déterminer sa valeur. Pour $d = \gcd(n + 1, 3n - 1)$, la combinaison $3(n + 1) - (3n - 1) = 4$ impose $d \mid 4$. Mieux, l'invariance des diviseurs

donne $d = \gcd(n+1, 4)$. Ainsi d=1 si n est pair, d=2 si $n \equiv 1 \pmod 4$, et d=4 si $n \equiv 3 \pmod 4$. Il faut distinguer les cas pour donner une réponse complète.

À toi d'essayer : Vérifier avant d'utiliser

Peut-on inverser 14 modulo 35 ? Et 14 modulo 15 ?
Pour démarrer. Un inverse exigerait une combinaison de 14 et du module égale à 1.

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

Indices, p. 28 Explication, p. 30

À toi d'essayer : Déterminer un PGCD variable

Calcule $\gcd(n, 2n+3)$ pour n entier positif.
Pour démarrer. Compare les diviseurs communs avant et après la soustraction $2n + 3 - 2n$.

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

Indices, p. 28 Explication, p. 31

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 — PGCD et signes ★☆☆

Calcule $\gcd(-18, 30)$, $\gcd(0, 27)$ et $\gcd(8, 15)$.

Exercice 2 — Euclide ★☆☆

Calcule $\gcd(414, 162)$.

Exercice 3 — Vérifier Bézout ★☆☆

Vérifie $35 \times (-1) + 12 \times 3 = 1$. Que peux-tu conclure ? Donne un inverse de 12 modulo 35.

Exercice 4 — Simplifier avec Gauss ★☆☆

Si $9 \mid 7n$, prouve que $9 \mid n$.

Exercice 5 — Inverse modulaire ★☆☆

Détermine un inverse de 7 modulo 20 et résous $7x \equiv 9 \pmod{20}$.

Exercice 6 — Remonter Euclide ★★☆

Trouve des entiers u,v tels que $37u + 26v = 1$.

Exercice 7 — Pas de solution ★★☆

Pourquoi $12x + 18y = 5$ n'a-t-elle aucune solution entière ?

Exercice 8 — Toutes les solutions ★★☆

Résous $7x + 5y = 1$ dans $\mathbb{Z}^2$.

Exercice 9 — Congruence non inversible ★★☆

Résous $8x \equiv 12 \pmod{20}$.

Exercice 10 — Combiner des divisibilités ★★☆

Si un entier n est divisible par 8 et par 9, montre qu'il est divisible par 72. L'analogue avec 6 et 9 donne-t-il 54 ?

Exercice 11 — Solutions positives ★★★

Une commande de 100 objets utilise des boîtes de 6 ou de 14 objets. Trouve les couples $(x, y) \in \mathbb{N}^2$ tels que $6x + 14y = 100$.

Exercice 12 — PGCD dépendant d'un entier ★★★

Pour $n \in \mathbb{N}$, détermine $\gcd(n + 2, 2n + 1)$.

Exercice 13 — Une fraction irréductible ⭐⭐⭐

Montre que $(2n+1)/(3n+2)$ est irréductible pour tout $n \in \mathbb{N}$.

Exercice 14 — Une racine rationnelle, prolongement ⭐⭐⭐

Soit $P(X) = X^3 - 2X + 2$. Si p/q est une racine rationnelle avec $q > 0$ et $\gcd(p,q) = 1$, montre que $q = 1$ et $p \mid 2$. Conclus.

Exercice 15 — Invariant de l'algorithme ⭐⭐⭐

Exécute `bezout(30, 18)` et explique le rôle des coefficients.

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.

Deux horloges et le théorème chinois

Deux signaux se déclenchent tous les 7 et 11 jours. On cherche un jour x congru à 3 modulo 7 et à 5 modulo 11. Le but est de résoudre ce cas puis de démontrer une règle générale. Durée indicative : 75 à 100 minutes.

Partie I — Résoudre à la main

1. Écris $x = 3 + 7k$ et déduis une congruence pour k modulo 11.
2. Trouve k puis toutes les valeurs de x. Donne la première valeur positive.
3. Pourquoi deux solutions diffèrent-elles d'un multiple de 77 ?

Partie II — Construire une solution générale

Soient $m, n \geq 2$ premiers entre eux et $mu + nv = 1$.

1. Pour deux entiers a,b, vérifie que $x_0 = anv + bmu$ satisfait $x_0 \equiv a \pmod{m}$ et $x_0 \equiv b \pmod{n}$.
2. Montre que toutes les solutions sont $x_0 + mnk$, $k \in \mathbb{Z}$.
3. Pourquoi y a-t-il un unique représentant dans $\{0, \ldots, mn - 1\}$?

Partie III — Lorsque les modules ne sont pas premiers entre eux

1. Montre que $x \equiv 1 \pmod{6}$ et $x \equiv 2 \pmod{9}$ sont incompatibles.
2. Résous en revanche $x \equiv 1 \pmod{6}$ et $x \equiv 4 \pmod{9}$.
3. Pour $d = \gcd(m, n)$, démontre que $a \equiv b \pmod{d}$ est une condition nécessaire à l'existence d'une solution.

Pistes

L'inverse de 7 modulo 11 est 8. Dans II, réduis séparément l'expression proposée modulo m et n. Dans III, commence par réduire les deux restes modulo 3.

7 Indices des exercices

Exercice 1

Travaille avec les valeurs absolues.

Zéro est divisible par tout entier non nul.

Exercice 2

Écris toutes les divisions successives.

Arrête-toi au reste nul, mais conserve le reste précédent.

Exercice 3

Une combinaison égale à 1 caractérise la coprimalité.

Réduis l'identité modulo 35.

Exercice 4

Vérifie le PGCD des deux coefficients.

Tu peux aussi produire une combinaison égale à 1.

Exercice 5

Cherche un petit multiple de 7 voisin d'un multiple de 20.

Multiplie ensuite toute la congruence par l'inverse.

Exercice 6

Isole chaque reste.

Remplace progressivement jusqu'à retrouver 37 et 26.

Exercice 7

Cherche un diviseur commun aux deux coefficients.

Compare ce diviseur au second membre.

Exercice 8

Trouve d'abord une solution particulière.

Les pas sont 5 pour x et -7 pour y.

Exercice 9

Divise coefficient, second membre et module par le PGCD.

Compte les quatre classes modulo 20.

Exercice 10

Vérifie la coprimalité avant de multiplier.

Cherche un petit contre-exemple dans le second cas.

Exercice 11

Commence par réduire l'équation.

Traduis ensuite les deux positivités en bornes sur k.

Exercice 12

Élimine n par combinaison linéaire.

Distingue les valeurs qui rendent les deux termes multiples de 3.

Exercice 13

Cherche une identité de Bézout indépendante de n.

Compare les coefficients 2 et 3.

Exercice 14

Multiplie par le cube du dénominateur.

Teste seulement les diviseurs de 2 une fois q=1 établi.

Exercice 15

Suis simultanément les restes et leurs expressions.

Chaque nouveau reste soustrait q fois la seconde ligne à la première.

8 Corrigés détaillés

Corrigé 1

Démonstration | Solution expliquée

Les diviseurs positifs d'un entier et de son opposé sont les mêmes. Donc $\gcd(-18, 30) = \gcd(18, 30) = 6$, puisque les diviseurs communs positifs sont $1, 2, 3, 6$. Pour $\gcd(0, 27)$, tout diviseur de 27 divise aussi 0 ; le plus grand est 27, donc le PGCD vaut 27.
Les diviseurs positifs de 8 sont $1, 2, 4, 8$ et ceux de 15 sont $1, 3, 5, 15$. Leur seule valeur commune est 1, donc le PGCD vaut 1. Cela n'affirme pas que 8 et 15 sont premiers : ils sont *premiers entre eux*.

Corrigé 2

Démonstration | Solution expliquée

Divisons successivement : $414 = 2 \times 162 + 90$, puis $162 = 1 \times 90 + 72$, puis $90 = 1 \times 72 + 18$, enfin $72 = 4 \times 18 + 0$. Les restes sont à chaque fois positifs ou nuls et inférieurs au diviseur.
Les couples $(414, 162), (162, 90), (90, 72), (72, 18), (18, 0)$ ont le même PGCD par l'étape d'Euclide. Le dernier vaut 18, donc le premier aussi. Contrôle : $414 = 18 \times 23$ et $162 = 18 \times 9$. Ces divisions vérifient que 18 est commun ; l'algorithme prouve en plus qu'il est le plus grand.

Corrigé 3

Démonstration | Solution expliquée

Calculons les deux produits : $35(-1) = -35$ et $12 \times 3 = 36$. Leur somme vaut 1. Tout diviseur commun de 35 et 12 divise donc 1 ; leur PGCD vaut 1 par Bézout.
Pour trouver l'inverse de 12 modulo 35, réduisons l'identité modulo 35 : le terme -35 a reste zéro, donc $12 \times 3 \equiv 1$. L'inverse est 3 modulo 35. On le vérifie directement : $36 = 35 + 1$. Le coefficient -1 placé devant 35 serait utile pour un inverse de 35 modulo 12, pas pour la question posée.

Corrigé 4

Démonstration | Solution expliquée

Nous voulons supprimer le facteur 7 dans $9 \mid 7n$. Vérifions d'abord la coprimalité : $1 = 4 \times 7 - 3 \times 9$, donc 7 et 9 sont premiers entre eux. Gauss s'applique et donne $9 \mid n$.
Pour voir concrètement le mécanisme, écrivons $7n = 9k$ avec $k \in \mathbb{Z}$. Multiplier l'identité par n donne $n = 4(7n) - 3(9n) = 4 \times 9k - 3 \times 9n = 9(4k - 3n)$. La parenthèse étant entière, cela prouve directement la divisibilité.

Corrigé 5

Démonstration | Solution expliquée

Le produit $7 \times 3 = 21 = 20 + 1$ montre que 3 est un inverse de 7 modulo 20. Multiplier toute la congruence $7x \equiv 9$ par 3 donne $21x \equiv 27$, donc $x \equiv 7 \pmod{20}$.

Les solutions sont $x = 7 + 20k$, $k \in \mathbb{Z}$. Vérification pour la famille : $7x - 9 = 49 + 140k - 9 = 20(2 + 7k)$, multiple de 20. Le passage par un inverse étant réversible, il n'y a pas d'autre classe de solutions.

Corrigé 6

Démonstration | Solution expliquée

Euclide donne $37 = 26 + 11$, $26 = 2 \times 11 + 4$, $11 = 2 \times 4 + 3$, $4 = 3 + 1$. Nous remontons depuis 1 en éliminant les restes :

$$\begin{aligned} 1 &= 4 - 3 = 4 - (11 - 2 \times 4) = 3 \times 4 - 11 \\ &= 3(26 - 2 \times 11) - 11 = 3 \times 26 - 7 \times 11 \\ &= 3 \times 26 - 7(37 - 26) = 10 \times 26 - 7 \times 37. \end{aligned}$$

Les coefficients demandés dans l'ordre $37u + 26v$ sont donc $u = -7, v = 10$. Contrôle : $37(-7) + 26(10) = -259 + 260 = 1$. Les parenthèses de la remontée empêchent de perdre le signe du terme soustrait.

Corrigé 7

Démonstration | Solution expliquée

Les coefficients sont $12 = 6 \times 2$ et $18 = 6 \times 3$. Pour des entiers x, y, le membre gauche s'écrit $6(2x + 3y)$: il est toujours divisible par 6. Or $5 = 6 \times 0 + 5$ ne l'est pas.
Une égalité imposerait donc que 5 soit un multiple de 6, contradiction. Il n'existe aucune solution entière. La valeur réelle $x = 5/12, y = 0$ satisfait l'égalité mais ne répond pas au problème, qui impose des coordonnées entières.

Corrigé 8

Démonstration | Solution expliquée

Le couple $(3, -4)$ convient : $7 \times 3 + 5(-4) = 21 - 20 = 1$. Prenons une autre solution et soustrayons cette identité : $7(x - 3) + 5(y + 4) = 0$. Ainsi $5 \mid 7(x - 3)$. Comme 5 et 7 sont premiers entre eux, Gauss donne $5 \mid (x - 3)$, donc $x = 3 + 5k$.
Remplacer dans l'égalité soustraite donne $35k + 5(y + 4) = 0$, donc $y = -4 - 7k$. Pour tout entier k, $7(3 + 5k) + 5(-4 - 7k) = 1$. Toutes les solutions ont cette forme et toutes les valeurs de k conviennent : la famille est exhaustive.

Corrigé 9

Démonstration | Solution expliquée

Le PGCD de 8 et 20 est 4 ; il divise 12, donc une résolution est possible. Écrivons $8x - 12 = 20k$. Diviser l'égalité par 4 donne $2x - 3 = 5k$, soit $2x \equiv 3 \pmod 5$.
Comme $2 \times 3 = 6 \equiv 1$, l'inverse de 2 est 3 modulo 5. Donc $x \equiv 9 \equiv 4 \pmod 5$, soit $x = 4 + 5t$. Pour $t = 0, 1, 2, 3$, les restes modulo 20 sont $4, 9, 14, 19$; un t augmenté de 4 répète un reste. Vérification : $8(4 + 5t) - 12 = 20 + 40t = 20(1 + 2t)$.

Corrigé 10

Démonstration | Solution expliquée

Écrivons $n = 8k$, puisque 8 divise n. Comme 9 divise aussi n, $9 \mid 8k$. Les entiers 8 et 9 sont premiers entre eux (leur différence vaut 1), donc Gauss donne $9 \mid k$. Alors $k = 9\ell$ et $n = 72\ell$: 72 divise bien n.
Pour 6 et 9, leur PGCD vaut 3, donc cette suppression de facteur n'est pas permise. Le nombre 18 fournit un contre-exemple : $18 = 6 \times 3 = 9 \times 2$, mais il n'est pas multiple de 54. Le plus petit multiple commun est ici $6 \times 9/3 = 18$.

Corrigé 11

Démonstration | Solution expliquée

Divisons l'équation par 2 : $3x + 7y = 50$. Modulo 3, elle devient $y \equiv 2$, puisque $7 \equiv 1$ et $50 \equiv 2$. Donc $y = 2 + 3k$. Substituer donne $3x + 14 + 21k = 50$, d'où $3x = 36 - 21k$ et $x = 12 - 7k$.
Les contraintes sont $2 + 3k \geq 0$, donc $k \geq -2/3$, soit $k \geq 0$ pour un entier ; et $12 - 7k \geq 0$, donc $k \leq 12/7$, soit $k \leq 1$. Ainsi $k = 0$ ou 1, donnant $(x, y) = (12, 2)$ ou $(5, 5)$. Contrôles : $6 \times 12 + 14 \times 2 = 72 + 28 = 100$ et $6 \times 5 + 14 \times 5 = 30 + 70 = 100$.

Corrigé 12

Démonstration | Solution expliquée

Tout diviseur commun de $n + 2$ et $2n + 1$ divise $2(n + 2) - (2n + 1) = 3$. Le PGCD positif est donc un diviseur de 3 : seulement 1 ou 3.
Pour qu'il vaille 3, il faut $n + 2 \equiv 0 \pmod 3$, donc $n \equiv 1 \pmod 3$. Cette condition suffit aussi : si $n = 3k + 1$, alors $n + 2 = 3(k + 1)$ et $2n + 1 = 6k + 3 = 3(2k + 1)$. Le PGCD est donc 3 dans ce cas, et 1 pour les deux autres restes de n. La combinaison réduit les possibilités, puis la réciproque permet de les départager.

Corrigé 13

Démonstration | Solution expliquée

Le dénominateur $3n + 2$ est au moins 2 pour $n \in \mathbb{N}$, donc la fraction est définie. Cherchons une combinaison annulant le terme en n : $3(2n + 1) - 2(3n + 2) = 6n + 3 - 6n - 4 = -1$.
Si un entier positif d divisait le numérateur et le dénominateur, il diviserait aussi -1, donc vaudrait 1. Leur PGCD est donc 1 : la fraction est irréductible. En changeant le signe de la combinaison, on obtient même une identité de Bézout égale à 1.

Corrigé 14

Démonstration | Solution expliquée

Supposons p/q racine, avec $q > 0$ et $\gcd(p, q) = 1$. Multiplier l'équation par q^3 donne $p^3 - 2pq^2 + 2q^3 = 0$, donc $p^3 = q^2(2p - 2q)$ et $q \mid p^3$. Gauss s'applique successivement avec le facteur p, premier avec q : de $q \mid p \cdot p^2$, on déduit $q \mid p^2$, puis $q \mid p$, puis $q \mid 1$. Comme $q > 0$, $q = 1$.

L'équation devient $p^3 - 2p + 2 = 0$, soit $2 = p(2 - p^2)$, donc $p \mid 2$. Les seuls candidats sont $1, -1, 2, -2$. Leurs images sont respectivement $1 - 2 + 2 = 1$, $-1 + 2 + 2 = 3$, $8 - 4 + 2 = 6$, $-8 + 4 + 2 = -2$. Aucune n'est nulle. Il n'y a donc aucune racine rationnelle.

Corrigé 15

Démonstration | Solution expliquée

Au départ, $r_0 = 30 = 1 \times 30 + 0 \times 18$ et $r_1 = 18 = 0 \times 30 + 1 \times 18$. Le quotient 1 donne le reste $12 = 30 - 18$, donc ses coefficients sont $(1, -1)$. Le quotient suivant est encore $1 : 6 = 18 - 12 = 18 - (30 - 18) = -30 + 2 \times 18$, coefficients $(-1, 2)$. Enfin $12 = 2 \times 6 + 0$ arrête l'algorithme.
Le dernier reste non nul et ses coefficients donnent $(6, -1, 2)$. Vérification : $30(-1) + 18 \times 2 = 6$.
À chaque ligne, la même opération « première ligne moins quotient fois seconde » est effectuée sur les restes et sur leurs coefficients. Ainsi l'algorithme conserve une expression exacte des restes avec les nombres de départ.

9 Corrigé du problème

Partie I — Transformer le système en une congruence

1. $x \equiv 3 \pmod 7$ signifie $x = 3+7k$ pour un entier k. Remplaçons dans la seconde condition : $3+7k \equiv 5 \pmod{11}$. Soustraire 3 donne $7k \equiv 2 \pmod{11}$.

2. Le produit $7 \times 8 = 56 = 5 \times 11 + 1$ montre que 8 est un inverse de 7 modulo 11. Multiplier donne $k \equiv 16 \equiv 5 \pmod{11}$. Donc $k = 5 + 11t$, puis $x = 3 + 7(5 + 11t) = 38 + 77t$. Pour $t = 0$, $x = 38$; pour $t \leq -1$, $x \leq -39$, et pour $t \geq 1$, $x \geq 115$. La première valeur positive est donc 38. Vérification : $38 = 5 \times 7 + 3 = 3 \times 11 + 5$.

3. Si x, x' satisfont les deux congruences, $x - x'$ est divisible par 7 et par 11. Écrivons $x - x' = 7h$. Comme 11 divise $7h$ et est premier avec 7, Gauss donne $h = 11s$. Donc $x - x' = 77s$. La période 77 vient de cette preuve, pas seulement des premiers jours essayés.

Partie II — Construire et prouver toutes les solutions

1. L'identité $mu+nv = 1$ donne, modulo m, $nv \equiv 1$ et $mu \equiv 0$. Ainsi $x_0 = anv+bmu \equiv a\times 1+b\times 0 = a$. Modulo n, les rôles s'échangent : $nv \equiv 0$, $mu \equiv 1$, donc $x_0 \equiv a \times 0 + b \times 1 = b$. Le choix des deux termes construit une contribution utile dans un module et nulle dans l'autre.

2. Pour toute solution x, les deux différences $x - x_0$ sont divisibles par m et par n. Comme ils sont premiers entre eux, leur produit divise la différence : $x = x_0 + mnk$. Réciproquement, ajouter un multiple de mn ajoute un multiple de chacun des modules ; toute valeur de cette forme conserve donc les deux congruences. Cela prouve l'exhaustivité et la validité de la famille.

3. La division euclidienne de x_0 par mn donne $x_0 = mnq + r$ avec $0 \leq r < mn$. Le reste $r = x_0 - mnq$ appartient à la famille et fournit un représentant dans l'intervalle. Si deux représentants y existaient, leur différence serait un multiple de mn strictement compris entre $-mn$ et mn, donc zéro. Le représentant est unique.

Partie III — Comprendre l'obstacle d'un diviseur commun

1. Si $x = 1 + 6k$, alors $x \equiv 1 \pmod 3$. Si $x = 2 + 9\ell$, alors $x \equiv 2 \pmod 3$. Un entier ne peut avoir deux restes différents dans la même division euclidienne : le premier système est impossible.

2. Pour le second, $x = 1 + 6k$ et $x \equiv 4 \pmod 9$ donnent $6k \equiv 3 \pmod 9$. Cela signifie $6k - 3 = 9\ell$. Diviser par 3 donne $2k-1 = 3\ell$, soit $2k \equiv 1 \pmod 3$. L'inverse de 2 modulo 3 est 2, donc $k \equiv 2 \pmod 3$, soit $k = 2 + 3t$. Ainsi $x = 1 + 6(2 + 3t) = 13 + 18t$. Contrôle : $x - 1 = 6(2 + 3t)$ et $x - 4 = 9(1 + 2t)$, donc les deux conditions sont satisfaites. La période est 18, PPCM de 6 et 9.

3. En général, $d = \gcd(m, n)$ divise m et n. Si $x - a = mk$ et $x - b = n\ell$, les deux différences sont divisibles par d. Leur soustraction donne $b - a = mk - n\ell$, encore divisible par d. Donc $a \equiv b \pmod d$ est nécessaire. Cette dernière preuve montre qu'une solution impose cette condition ; elle ne prétend pas à elle seule construire une solution lorsque la condition est satisfaite.

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 équation entière jusqu'au bout

Résous $4x + 7y = 1$ dans les entiers. Déduis un inverse de 4 modulo 7 et les solutions positives ou nulles.

Pour démarrer. Après le couple $(2, -1)$, soustrais les équations pour trouver les pas de la famille.

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

Indices, p. 28 Explication, p. 31

11 Fiche-mémoire

— Euclide : $\gcd(a,b) = \gcd(b,r)$; le dernier reste non nul est le PGCD.
— Bézout : $au + bv = d$; une combinaison égale à 1 caractérise les entiers premiers entre eux.
— Gauss : $a \mid bc$ et $\gcd(a,b) = 1$ impliquent $a \mid c$.
— a est inversible modulo n exactement si $\gcd(a,n) = 1$.
— $ax + by = c$ est soluble exactement si $d \mid c$; les solutions s'obtiennent par un paramètre entier.
— Pour $ax \equiv b \pmod{n}$, divise les trois termes par le PGCD lorsque celui-ci divise b.

Contrôle. Ai-je vérifié une identité de Bézout ? La coprimalité exigée par Gauss est-elle établie ? Mon paramètre est-il entier ? Ai-je imposé les éventuelles contraintes de positivité à la fin ?

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.

Premiers entre eux ne veut pas dire premiers

Indice 1 — Une piste.

Liste les diviseurs positifs de 8.

Indice 2 — Un pas de plus.

Compare les listes, pas seulement la parité.

Revenir à la recherche, p. 4

Lire la dernière ligne

Indice 1 — Une piste.

Commence par $84 = 2 \times 30 + 24$.

Indice 2 — Un pas de plus.

Puis divise 30 par 24, et 24 par le nouveau reste.

Revenir à la recherche, p. 5

Fabriquer le 1 qui permet de simplifier

Indice 1 — Une piste.

Isole le dernier reste non nul.

Indice 2 — Un pas de plus.

Remplace 3 dans $1 = 7 - 2 \times 3$.

Revenir à la recherche, p. 7

Construire la simplification

Indice 1 — Une piste.

Cherche une combinaison de 7 et 3 égale à 1.

Indice 2 — Un pas de plus.

Utilise $1 = 7 - 2 \times 3$, puis multiplie par n.

Revenir à la recherche, p. 8

Vérifier avant de supprimer un facteur

Indice 1 — Une piste.

Compare les PGCD de 15 avec 4 puis avec 5.

Indice 2 — Un pas de plus.

Pour réfuter la seconde implication, cherche un petit n.

Revenir à la recherche, p. 8

Utiliser le bon coefficient de Bézout

Indice 1 — Une piste.

Le coefficient placé devant 7 est son inverse modulo 17.

Indice 2 — Un pas de plus.

Multiplie les deux membres de la congruence par 5.

Revenir à la recherche, p. 9

Passer d'un couple à tous les couples

Indice 1 — Une piste.

Le couple $(2, -1)$ est une solution particulière.

Indice 2 — Un pas de plus.

Écris $x = 2 + 5k$ et $y = -1 - 3k$.

Revenir à la recherche, p. 10

PGCD ou PPCM selon la question

Indice 1 — Une piste.

Cherche un multiple commun positif, pas un diviseur.

Indice 2 — Un pas de plus.

Le PGCD vaut 6 et le produit vaut 216.

Revenir à la recherche, p. 12

Vérifier avant d'utiliser

Indice 1 — Une piste.

Compare les deux PGCD.

Indice 2 — Un pas de plus.

Modulo 15, 14 est congru à -1.

Revenir à la recherche, p. 13

Déterminer un PGCD variable

Indice 1 — Une piste.

Soustrais deux fois n au second terme.

Indice 2 — Un pas de plus.

Le PGCD est celui de n et 3.

Revenir à la recherche, p. 13

Une équation entière jusqu'au bout

Indice 1 — Une piste.

Le couple $(2, -1)$ convient.

Indice 2 — Un pas de plus.

Toutes les solutions sont $(2 + 7k, -1 - 4k)$.

Revenir à la recherche, p. 24

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.

Premiers entre eux ne veut pas dire premiers

Les diviseurs positifs de 8 sont $1, 2, 4, 8$; ceux de 9 sont $1, 3, 9$. Leur seule valeur commune est 1, donc leur PGCD vaut 1 : 8 et 9 sont premiers entre eux. Ceux de 12 sont $1, 2, 3, 4, 6, 12$. Avec 8, les valeurs communes sont $1, 2, 4$, donc le PGCD vaut 4. Les nombres 8 et 9 sont pourtant composés, puisqu'ils ont des diviseurs autres que 1 et eux-mêmes. « Premiers entre eux » est une relation entre deux nombres, pas une propriété individuelle de chacun.

Revenir à la recherche, p. 4

Lire la dernière ligne

$84 = 2 \times 30 + 24$, donc le PGCD est celui de 30 et 24. Puis $30 = 1 \times 24 + 6$, donc celui de 24 et 6. Enfin $24 = 4 \times 6 + 0$, donc celui de 6 et 0, égal à 6. Les restes étaient $24, 6, 0$; le dernier non nul est 6. Vérification : $84 = 6 \times 14$ et $30 = 6 \times 5$. Les diviseurs communs sont tous les diviseurs de 6, soit $1, 2, 3, 6$ si on les demande positifs ; le PGCD ne désigne que le plus grand.

Revenir à la recherche, p. 5

Fabriquer le 1 qui permet de simplifier

La seconde division donne $1 = 7 - 2 \times 3$. La première donne $3 = 17 - 2 \times 7$. Substituer en conservant les parenthèses donne $1 = 7 - 2(17 - 2 \times 7) = 7 - 2 \times 17 + 4 \times 7 = 5 \times 7 - 2 \times 17$. Vérification : $35 - 34 = 1$. Les coefficients de 17 et 7 sont respectivement -2 et 5. Cette identité prouve leur coprimalité, car tout diviseur commun diviserait 1. Elle fournit aussi l'inverse 5 de 7 modulo 17.

Revenir à la recherche, p. 7

Construire la simplification

L'hypothèse signifie $3n = 7k$ pour un entier k. Puisque $7 - 2 \times 3 = 1$, multiplier par n donne $n = 7n - 2(3n)$. Remplaçons $3n$ par $7k$: $n = 7n - 14k = 7(n - 2k)$. Le nombre $n - 2k$ est entier, donc 7 divise n. Le calcul montre le quotient entier qui justifie la conclusion ; il ne se contente pas de supprimer le facteur 3 dans la divisibilité initiale.

Revenir à la recherche, p. 8

Vérifier avant de supprimer un facteur

Les diviseurs de 15 sont $1, 3, 5, 15$; aucun sauf 1 ne divise 4, donc $\gcd(15, 4) = 1$. Gauss donne $15 \mid n$ à partir de $15 \mid 4n$. On peut voir l'identité $1 = 4 \times 4 - 15$, donc $n = 4(4n) - 15n$, multiple de 15. Avec le facteur 5, le PGCD vaut 5 et non 1. Pour $n = 3$, $5n = 15$ est divisible par 15, mais $n = 3$ ne l'est pas. Cet exemple prouve que la seconde implication est fausse.

Revenir à la recherche, p. 8

Utiliser le bon coefficient de Bézout

Dans $1 = 5 \times 7 - 2 \times 17$, le second terme est multiple de 17. Il reste $5 \times 7 \equiv 1 \pmod{17}$: l'inverse de 7 est donc 5. Multiplier $7x \equiv 3$ par 5 donne $x \equiv 15 \pmod{17}$. La famille est $x = 15 + 17k$. Pour la contrôler, $7x - 3 = 105 + 119k - 3 = 17(6 + 7k)$, bien multiple de 17. Le coefficient -2 accompagne le module ; ce n'est pas l'inverse demandé.

Revenir à la recherche, p. 9

Passer d'un couple à tous les couples

Le couple $(2, -1)$ vérifie $6 - 5 = 1$. Pour toute autre solution, $3(x - 2) + 5(y + 1) = 0$, donc $5 \mid 3(x - 2)$. Comme 3 et 5 sont premiers entre eux, $x - 2 = 5k$. Alors $3 \times 5k + 5(y + 1) = 0$, donc $y = -1 - 3k$. Toute la famille $(2 + 5k, -1 - 3k)$ redonne 1. Pour la positivité, $k \geq -2/5$ impose $k \geq 0$, et $k \leq -1/3$ impose $k \leq -1$, car k est entier. Ces deux conditions sont incompatibles : aucune solution positive ou nulle.

Revenir à la recherche, p. 10

PGCD ou PPCM selon la question

Les jours du premier événement sont les multiples de 12 ; ceux du second les multiples de 18. La première rencontre après aujourd'hui est donc le plus petit multiple commun positif. Euclide donne $18 = 12 + 6$ puis $12 = 2 \times 6$, donc le PGCD vaut 6. Le PPCM vaut $12 \times 18/6 = 36$. Vérification : $36 = 3 \times 12 = 2 \times 18$. Le jour 6 ne conviendrait pas, car ce n'est un multiple ni de 12 ni de 18 ; le PGCD est utilisé dans le calcul, mais n'est pas la période de rencontre.

Revenir à la recherche, p. 12

Vérifier avant d'utiliser

Le PGCD de 14 et 35 vaut 7. Si $14u \equiv 1 \pmod{35}$, il existerait v tel que $14u + 35v = 1$. Le membre gauche serait divisible par 7, le droit ne l'est pas : impossible. Modulo 15, $14 \equiv -1$, donc $14^2 \equiv (-1)^2 = 1$. Ainsi 14 est son propre inverse modulo 15. Vérification entière : $196 = 13 \times 15 + 1$. L'existence de l'inverse dépend du module, pas du seul nombre 14.

Revenir à la recherche, p. 13

Déterminer un PGCD variable

Un diviseur commun à n et $2n+3$ divise aussi $2n+3-2n=3$. Inversement, un diviseur commun à n et 3 divise $2n+3$. Les ensembles de diviseurs communs sont donc identiques et le PGCD est $\gcd(n,3)$. Comme 3 est premier, il vaut 3 si 3 divise n, sinon 1. Ces deux sens sont nécessaires : la seule combinaison montrerait que le PGCD divise 3, sans suffire à conclure dans chaque cas.

Revenir à la recherche, p. 13

Une équation entière jusqu'au bout

$4\times 2+7(-1)=1$. Pour une autre solution, $4(x-2)+7(y+1)=0$. Gauss donne $7 \mid (x-2)$, car $\gcd(4,7)=1$. Écrivons $x=2+7k$; remplacer donne $y=-1-4k$. Toute cette famille vérifie $4x+7y=8+28k-7-28k=1$. Modulo 7, l'identité particulière donne $4\times 2\equiv 1$, donc 2 est un inverse de 4. Pour $x,y\geq 0$, on aurait $k\geq -2/7$, donc $k\geq 0$, et $k\leq -1/4$, donc $k\leq -1$. Aucune valeur entière ne satisfait les deux.

Revenir à la recherche, p. 24