Plaquette 3 – Coefficients de Bézout et inverses modulaires

PGCD, théorème de Bézout, Gauss — Terminale maths expertes

Corrections détaillées

Boîte à outils

Théorèmes et méthodes.

— **Identité de Bézout** : pour tous entiers a et b non nuls, il existe des entiers u et v tels que

$$au + bv = \text{pgcd}(a\,;b)$$

— **Théorème de Bézout** : a et b sont **premiers entre eux** si et seulement s'il existe u, v entiers tels que $au + bv = 1$. Une seule identité suffit à conclure.

— **Méthode de la remontée** : on écrit les divisions d'Euclide, on isole le dernier reste non nul, puis on remplace **de bas en haut** chaque reste par son expression, sans jamais calculer les produits — on garde a et b apparents.

— **Inverse modulaire** : a possède un inverse modulo n si et seulement si $\text{pgcd}(a\,;n) = 1$. L'identité $au + nv = 1$ donne $au \equiv 1 \pmod{n}$: l'inverse est u (réduit modulo n).

— **Résolution de** $ax \equiv b \pmod{n}$ lorsque $\text{pgcd}(a\,;n) = 1$: on multiplie par l'inverse, $x \equiv a^{-1}b \pmod{n}$. La solution est **une seule classe** modulo n.

— **Si** $\text{pgcd}(a\,;n) = d > 1$: l'équation n'a de solutions que si $d \mid b$; on divise alors a, b **et** n par d, et on obtient d classes solutions modulo n.

— **Les couples de Bézout ne sont pas uniques** : si $(u_0\,;v_0)$ convient pour $au + bv = 1$, alors $(u_0 + kb\,;v_0 - ka)$ convient aussi, pour tout $k \in \mathbb{Z}$.

Correction de l'exercice 1 – Remonter l'algorithme d'Euclide

a) On déroule l'algorithme d'Euclide en **gardant chaque ligne écrite** : c'est elle qui servira à la remontée.

— $45 = 32 \times 1 + 13$
— $32 = 13 \times 2 + 6$
— $13 = 6 \times 2 + 1$
— $6 = 1 \times 6 + 0$
— Le dernier reste non nul est 1 : $\text{pgcd}(45\,;32) = 1$, les deux nombres sont premiers entre eux.

b) On part de l'avant-dernière ligne, celle qui **isole le** 1, puis on remonte.

— $1 = 13 - 2 \times 6$
— On remplace $6 = 32 - 2 \times 13$: $1 = 13 - 2(32 - 2 \times 13) = 5 \times 13 - 2 \times 32$.
— On remplace $13 = 45 - 32$: $1 = 5(45 - 32) - 2 \times 32 = 5 \times 45 - 7 \times 32$.

Vérification : $5 \times 45 - 7 \times 32 = 225 - 224 = 1$ ✓.

— **Conclusion** : $(u\,;v) = (5\,;-7)$ convient.
— **Le geste à ne pas rater** : ne jamais effectuer les produits pendant la remontée, sinon on perd 45 et 32 de vue.

Réponse. $5 \times 45 - 7 \times 32 = 1$, donc $(u\,;v) = (5\,;-7)$.

Correction de l'exercice 2 – Bézout avec un PGCD non trivial

a) Algorithme d'Euclide :

— $1\,071 = 462 \times 2 + 147$
— $462 = 147 \times 3 + 21$
— $147 = 21 \times 7 + 0$
— Le PGCD est 21.

b) On isole 21 dans l'avant-dernière ligne, puis on remonte :

— $21 = 462 - 3 \times 147$
— On remplace $147 = 1\,071 - 2 \times 462$:
— $21 = 462 - 3(1\,071 - 2 \times 462) = 462 - 3 \times 1\,071 + 6 \times 462 = 7 \times 462 - 3 \times 1\,071$.

Vérification : $7 \times 462 = 3\,234$ et $3 \times 1\,071 = 3\,213$, donc $3\,234 - 3\,213 = 21$ ✓.

— **Conclusion** : $(u\,;v) = (-3\,;7)$.
— Remarque : en divisant tout par 21, on obtient $7 \times 22 - 3 \times 51 = 1$ — une identité de Bézout pour 51 et 22, qui sont premiers entre eux.

Réponse. a) 21 · b) $(-3) \times 1\,071 + 7 \times 462 = 21$.

Correction de l'exercice 3 – Démontrer avec le théorème de Bézout

Le **théorème de Bézout** dit qu'il suffit d'exhiber **une** combinaison linéaire égale à 1.

— On cherche à éliminer n : on multiplie le premier par 3, le second par 2.
— $3(2n + 3) = 6n + 9$ et $2(3n + 4) = 6n + 8$.
— Par différence : $3(2n + 3) - 2(3n + 4) = 1$.

$$3 \times (2n + 3) + (-2) \times (3n + 4) = 1$$

— C'est une identité de Bézout avec $u = 3$ et $v = -2$, valable pour **tout** entier n.
— D'après le théorème de Bézout, $\text{pgcd}(2n + 3\,;3n + 4) = 1$.
— Contrôle : $n = 5$ donne 13 et 19 ✓ ; $n = 10$ donne 23 et 34 ✓.
— **À retenir** : pour démontrer « premiers entre eux », l'identité de Bézout est plus rapide que l'algorithme d'Euclide, qui ne s'applique pas à des expressions littérales.

Réponse. $3(2n + 3) - 2(3n + 4) = 1$: théorème de Bézout.

Correction de l'exercice 4 – Tous les couples de Bézout

a) Les nombres sont petits : on trouve un couple de tête.

— $5 \times 2 = 10$ et $3 \times 3 = 9$, donc $5 \times 2 + 3 \times (-3) = 10 - 9 = 1$.
— Le couple $(2\,;-3)$ convient.

b) Soit $(u\,;v)$ un autre couple solution. On soustrait les deux égalités :

— $5u + 3v = 1$ et $5 \times 2 + 3 \times (-3) = 1$, donc $5(u - 2) + 3(v + 3) = 0$.
— Soit $5(u - 2) = -3(v + 3)$: 3 divise $5(u - 2)$, et comme 3 et 5 sont premiers entre eux, le **théorème de Gauss** donne $3 \mid (u - 2)$.
— Donc $u - 2 = 3k$, soit $u = 2 + 3k$, et en reportant : $5 \times 3k = -3(v + 3)$, d'où $v = -3 - 5k$.

Conclusion. Les solutions sont les couples $(2 + 3k\,;-3 - 5k)$, $k \in \mathbb{Z}$.

— Vérification pour $k = 1$: $5 \times 5 + 3 \times (-8) = 25 - 24 = 1$ ✓.
— **Une identité de Bézout n'est donc jamais unique** : c'est normal d'obtenir un couple différent de celui du corrigé.

Réponse. $(u\,;v) = (2 + 3k\,;-3 - 5k)$, $k \in \mathbb{Z}$.

Correction de l'exercice 5 – Calculer un inverse modulaire

Existence : 43 est premier et ne divise pas 17, donc pgcd(17 ; 43) = 1 et l'inverse existe.

Algorithme d'Euclide :

— $43 = 17 \times 2 + 9$
— $17 = 9 \times 1 + 8$
— $9 = 8 \times 1 + 1$

Remontée :

— $1 = 9 - 8$
— $8 = 17 - 9$ donne $1 = 9 - (17 - 9) = 2 \times 9 - 17$.
— $9 = 43 - 2 \times 17$ donne $1 = 2(43 - 2 \times 17) - 17 = 2 \times 43 - 5 \times 17$.

On lit la congruence modulo 43 :

— $2 \times 43 \equiv 0$, donc $-5 \times 17 \equiv 1 \pmod{43}$, c'est-à-dire $17 \times (-5) \equiv 1$.
— On ramène dans $\{0 ; \dots ; 42\}$: $-5 \equiv 38 \pmod{43}$.
— **Vérification** : $17 \times 38 = 646 = 43 \times 15 + 1$ ✓.

Réponse. $17^{-1} \equiv 38 \pmod{43}$.

Correction de l'exercice 6 – Résoudre grâce à l'inverse

Tester les 43 classes serait interminable : on utilise l'inverse calculé à l'exercice précédent.

— $17^{-1} \equiv 38 \pmod{43}$.
— On multiplie les deux membres par 38 : $x \equiv 38 \times 5 = 190 \pmod{43}$.
— $190 = 43 \times 4 + 18$, donc $x \equiv 18 \pmod{43}$.

Vérification. $17 \times 18 = 306$ et $306 = 43 \times 7 + 5$ ✓.

— **Conclusion** : l'ensemble des solutions est $\{18 + 43k,\ k \in \mathbb{Z}\}$ — **une seule classe**, puisque 17 et 43 sont premiers entre eux.
— Variante de rédaction : partir de $2 \times 43 - 5 \times 17 = 1$, multiplier par 5, et lire $17 \times (-25) \equiv 5$, d'où $x \equiv -25 \equiv 18 \pmod{43}$ ✓.

Réponse. $x \equiv 18 \pmod{43}$.

Correction de l'exercice 7 – Déchiffrer un message affine

a) Le chiffrement est déchiffrable si 7 est inversible modulo 26, donc si pgcd(7 ; 26) = 1.

— $26 = 7 \times 3 + 5$; $7 = 5 \times 1 + 2$; $5 = 2 \times 2 + 1$: le PGCD vaut 1 ✓.
— Remontée : $1 = 5 - 2 \times 2 = 5 - 2(7 - 5) = 3 \times 5 - 2 \times 7$, puis $5 = 26 - 3 \times 7$ donne

$$1 = 3(26 - 3 \times 7) - 2 \times 7 = 3 \times 26 - 11 \times 7$$

— Donc $7 \times (-11) \equiv 1 \pmod{26}$, et $-11 \equiv 15$: l'inverse de 7 est 15.
— Vérification : $7 \times 15 = 105 = 26 \times 4 + 1$ ✓.

b) De $y \equiv 7x + 4$ on tire $7x \equiv y - 4$, puis $x \equiv 15(y - 4) \pmod{26}$.

Lettre	L	G	X	Y	O	H
y	11	6	23	24	14	7
$y-4$	7	2	19	20	10	3
$x = 15(y-4)$	1	4	25	14	20	19
Lettre claire	B	E	Z	O	U	T

— Détail : $15 \times 7 = 105 \equiv 1 \pmod{26}$; $15 \times 19 = 285 = 26 \times 10 + 25$, donc $x = 25$, la lettre Z.
— Le message est **BEZOUT**.

Réponse. a) $7^{-1} \equiv 15 \pmod{26}$ · b) BEZOUT.

Correction de l'exercice 8 – Un inverse par simple lecture

a) $45 \times 45 = 2\,025$, donc $2\,026 = 45 \times 45 + 1$ ✓ : l'algorithme d'Euclide s'arrête **dès la première division**.

— On en tire l'identité de Bézout : $1 = 2\,026 - 45 \times 45$, c'est-à-dire $1 = 1 \times 2\,026 + (-45) \times 45$.
— Modulo 2 026 : $45 \times (-45) \equiv 1$, donc l'inverse de 45 est $-45 \equiv 2\,026 - 45 = 1\,981$.
— **Vérification** : $45 \times 1\,981 = 89\,145$ et $2\,026 \times 44 = 89\,144$, donc le reste est bien 1 ✓.

b) On multiplie par l'inverse :

— $x \equiv 1\,981 \times 7 = 13\,867 \pmod{2\,026}$.
— $2\,026 \times 6 = 12\,156$ et $13\,867 - 12\,156 = 1\,711$, donc $x \equiv 1\,711 \pmod{2\,026}$.
— Vérification : $45 \times 1\,711 = 76\,995$, et $2\,026 \times 38 = 76\,988$, reste 7 ✓.
— **Plus élégant** : $45x \equiv 7$ donne, en multipliant par -45, $x \equiv -315 \equiv 2\,026 - 315 = 1\,711$ ✓.

Réponse. a) $45^{-1} \equiv 1\,981 \pmod{2\,026}$ · b) $x \equiv 1\,711 \pmod{2\,026}$.

Correction de l'exercice 9 – Un module non premier

a) $30 = 2 \times 3 \times 5$ et 11 est premier : $\gcd(11\,;30) = 1$, l'inverse existe même si 30 n'est pas premier.

— $30 = 11 \times 2 + 8$; $11 = 8 + 3$; $8 = 3 \times 2 + 2$; $3 = 2 + 1$.
— Remontée : $1 = 3 - 2 = 3 - (8 - 2 \times 3) = 3 \times 3 - 8$.
— Puis $3 = 11 - 8$: $1 = 3(11 - 8) - 8 = 3 \times 11 - 4 \times 8$.
— Enfin $8 = 30 - 2 \times 11$: $1 = 3 \times 11 - 4(30 - 2 \times 11) = 11 \times 11 - 4 \times 30$.
— Donc $11 \times 11 \equiv 1 \pmod{30}$: 11 est **son propre inverse**.
— Vérification : $121 = 30 \times 4 + 1$ ✓.

b) On multiplie par 11 :

— $x \equiv 11 \times 7 = 77 \pmod{30}$, et $77 = 60 + 17$, donc $x \equiv 17 \pmod{30}$.
— Vérification : $11 \times 17 = 187 = 30 \times 6 + 7$ ✓.

Réponse. a) $11^{-1} \equiv 11 \pmod{30}$ · b) $x \equiv 17 \pmod{30}$.

Correction de l'exercice 10 – Quand l'inverse n'existe pas

a) $\gcd(6\,;22) = 2 \neq 1$.

— Si 6 avait un inverse a, on aurait $6a \equiv 1 \pmod{22}$, donc $6a - 1 = 22k$, soit $6a - 22k = 1$.

— Or 2 divise $6a$ et $22k$, donc 2 diviserait 1 : impossible.
— 6 n'est donc pas inversible modulo 22 — pas plus qu'aucun nombre pair.

b) On ne peut pas multiplier par un inverse, mais 2 divise 6, 4 **et** 22 : on simplifie tout.

— $6x \equiv 4 \pmod{22}$ signifie $22 \mid (6x-4)$, soit $6x - 4 = 22k$.
— En divisant par 2 : $3x - 2 = 11k$, c'est-à-dire $3x \equiv 2 \pmod{11}$.
— 3 est inversible modulo 11 : $3 \times 4 = 12 \equiv 1$, donc $3^{-1} \equiv 4$.
— $x \equiv 4 \times 2 = 8 \pmod{11}$.

Conclusion. $x \equiv 8 \pmod{11}$, soit modulo 22 : $x \equiv 8$ ou $x \equiv 19$.

— Vérification : $6 \times 8 = 48 = 44 + 4$ ✓ et $6 \times 19 = 114 = 110 + 4$ ✓.
— **La règle** : $ax \equiv b \pmod{n}$ a des solutions si et seulement si $\gcd(a\,;n)$ divise b, et il y a alors exactement $\gcd(a\,;n)$ classes solutions.

Réponse. a) $\gcd(6\,;22) = 2$ · b) $x \equiv 8$ ou $19 \pmod{22}$.

Correction de l'exercice 11 – Un système par Bézout

Étape 1 : l'identité de Bézout. $9 = 7 + 2$; $7 = 2 \times 3 + 1$, donc

— $1 = 7 - 3 \times 2 = 7 - 3(9-7) = 4 \times 7 - 3 \times 9$.
— Vérification : $28 - 27 = 1$ ✓.

Étape 2 : construire une solution. On pose

$$x_0 = 5 \times (4 \times 7) + 2 \times (-3 \times 9) = 5 \times 28 - 2 \times 27 = 140 - 54 = 86$$

— Pourquoi ça marche : modulo 7, le premier terme disparaît et $-3 \times 9 \equiv 1$, donc $x_0 \equiv 2$ ✓.
— Modulo 9, le second terme disparaît et $4 \times 7 \equiv 1$, donc $x_0 \equiv 5$ ✓.

Étape 3 : conclure. $86 = 63 + 23$, donc $x_0 \equiv 23 \pmod{63}$.

— L'ensemble des solutions est $x \equiv 23 \pmod{63}$, avec $63 = 7 \times 9$.
— **Vérification** : $23 = 7 \times 3 + 2$ ✓ et $23 = 9 \times 2 + 5$ ✓.

Réponse. $x \equiv 23 \pmod{63}$.

Correction de l'exercice 12 – Un PGCD à discuter

a) On fait apparaître un reste constant par division :

$$n^2 + n + 1 = (n+2)(n-1) + 3$$

— Vérification : $(n+2)(n-1) = n^2 + n - 2$, et $+3$ donne bien $n^2 + n + 1$ ✓.
— d divise $n+2$, donc il divise $(n+2)(n-1)$; comme il divise aussi $n^2 + n + 1$, il divise la différence, c'est-à-dire 3.
— Donc $d \in \{1\,;3\}$.

b) $d = 3$ exactement quand 3 divise $n+2$, c'est-à-dire $n \equiv 1 \pmod{3}$.

— Si $n \equiv 1 \pmod{3}$: $n + 2 \equiv 0$, et $n^2 + n + 1 \equiv 1 + 1 + 1 = 3 \equiv 0 \pmod{3}$: les deux sont divisibles par 3, donc $d = 3$.
— Sinon, 3 ne divise pas $n+2$, donc $d = 1$.

Contrôle. $n = 4$: $\gcd(21\,;6) = 3$ ✓ ($4 \equiv 1 \pmod{3}$) · $n = 5$: $\gcd(31\,;7) = 1$ ✓.

Réponse. a) $d \mid 3$ · b) $d = 3$ si et seulement si $n \equiv 1 \pmod{3}$, sinon $d = 1$.

Correction de l'exercice 13 – Mesurer un litre

Traduction mathématique. Toute quantité obtenue est de la forme $5u + 3v$: u compte les remplissages (ou vidages) du récipient de 5 L, v ceux du récipient de 3 L.

— $\text{pgcd}(5\,;3) = 1$, donc d'après le théorème de Bézout, il existe u, v tels que $5u + 3v = 1$: la quantité 1 L est atteignable.

— Une identité : $5 \times 2 - 3 \times 3 = 10 - 9 = 1$.

— **Lecture concrète** : verser **deux** fois le récipient de 5 L et retirer **trois** fois celui de 3 L.

Le protocole correspondant, étape par étape :

Étape	Récipient de 5 L	Récipient de 3 L
Remplir le 5 L	5	0
Verser dans le 3 L	2	3
Vider le 3 L	2	0
Transvaser	0	2
Remplir le 5 L	5	2
Compléter le 3 L	4	3
Vider le 3 L, transvaser	1	3

— Bilan : on a rempli **deux** fois le récipient de 5 L (10 L entrés) et vidé **trois** fois celui de 3 L (9 L sortis), soit $10 - 9 = 1$ L restant — exactement le contenu de l'identité de Bézout.

— **Généralisation** : avec des récipients de a L et b L, les quantités mesurables sont exactement les multiples de $\text{pgcd}(a\,;b)$. Avec 4 L et 6 L, jamais 1 L.

Réponse. $5 \times 2 - 3 \times 3 = 1$: deux remplissages du 5 L, trois vidages du 3 L.

Correction de l'exercice 14 – Premier avec a et avec b, donc avec ab

a) On procède en deux temps, en n'utilisant que des combinaisons linéaires.

Étape 1 : $a + b$ est premier avec a, et avec b.

— Un diviseur commun de $a + b$ et de a divise la différence $(a + b) - a = b$: c'est donc un diviseur commun de a et b, donc il divise $\text{pgcd}(a\,;b) = 1$.

— Donc $\text{pgcd}(a + b\,;a) = 1$, et de même $\text{pgcd}(a + b\,;b) = 1$.

Étape 2 : on multiplie deux identités de Bézout.

— Il existe u, v, u', v' entiers tels que $(a + b)u + av = 1$ et $(a + b)u' + bv' = 1$.

— En multipliant membre à membre :

$$1 = [(a + b)u + av][(a + b)u' + bv'] = (a + b) \times K + ab \times (vv')$$

où $K = (a + b)uu' + ubv' + u'av$ est un entier.

— On obtient une identité de Bézout entre $a + b$ et ab : d'après le théorème de Bézout, ils sont premiers entre eux.

— **Conclusion** : $\text{pgcd}(a + b\,;ab) = 1$.

b) $a = 4$ et $b = 9$ sont premiers entre eux.

— $a + b = 13$ et $ab = 36$: $\text{pgcd}(13\,;36) = 1$ ✓ (13 est premier et ne divise pas 36).

— **Contre-exemple si l'hypothèse tombe** : $a = 4$, $b = 6$ donnent $a + b = 10$ et $ab = 24$, de PGCD 2.

Réponse. $a+b$ est premier avec a et avec b, donc avec ab.

Correction de l'exercice 15 – Bilan : Bézout de bout en bout

a) Algorithme d'Euclide :

— $31 = 17 \times 1 + 14$; $17 = 14 \times 1 + 3$; $14 = 3 \times 4 + 2$; $3 = 2 \times 1 + 1$.
— Remontée : $1 = 3 - 2 = 3 - (14 - 4 \times 3) = 5 \times 3 - 14$.
— $3 = 17 - 14$: $1 = 5(17 - 14) - 14 = 5 \times 17 - 6 \times 14$.
— $14 = 31 - 17$: $1 = 5 \times 17 - 6(31 - 17) = 11 \times 17 - 6 \times 31$.
— **Vérification** : $187 - 186 = 1$ ✓. Donc $(u\,;v) = (-6\,;11)$.

b) Modulo 31, l'identité donne $17 \times 11 \equiv 1$: l'inverse de 17 est 11.

— $17x \equiv 9$ donne $x \equiv 11 \times 9 = 99 \pmod{31}$.
— $99 = 31 \times 3 + 6$, donc $x \equiv 6 \pmod{31}$.
— Vérification : $17 \times 6 = 102 = 31 \times 3 + 9$ ✓.

c) Les quantités mesurables sont les multiples de pgcd des deux contenances.

— $\text{pgcd}(7\,;4) = 1$: oui, 1 L est mesurable. Une identité : $2 \times 4 - 1 \times 7 = 1$ — remplir deux fois le 4 L et retirer une fois le 7 L.
— $\text{pgcd}(6\,;9) = 3$: toute quantité obtenue est un multiple de 3 L, donc 1 L est **impossible**.

Réponse. a) $(-6\,;11)$ · b) $17^{-1} \equiv 11$, $x \equiv 6 \pmod{31}$ · c) oui avec 7 et 4 ; non avec 6 et 9.