Plaquette 1 – Euclide, identité de Bézout et équations diophantiennes

PGCD, Bézout et Gauss — Terminale maths expertes

Corrections détaillées

Boîte à outils

Théorèmes du cours.

— **Algorithme d'Euclide** : $\text{pgcd}(a\,;b) = \text{pgcd}(b\,;r)$ où r est le reste de a par b. Le PGCD est le **dernier reste non nul**.
— Propriété : $\text{pgcd}(a\,;b)$ divise toute combinaison $au + bv$.
— **Identité de Bézout** : il existe des entiers u, v tels que

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

On les obtient en **remontant** l'algorithme d'Euclide.

— **Théorème de Bézout** : a et b sont **premiers entre eux** si et seulement s'il existe u, v entiers tels que $au + bv = 1$.
— **Théorème de Gauss** : si $a \mid bc$ et si $\text{pgcd}(a\,;b) = 1$, alors $a \mid c$.
— Conséquence : si $b \mid n$, $c \mid n$ et $\text{pgcd}(b\,;c) = 1$, alors $bc \mid n$.
— **Équation diophantienne** $ax + by = c$: elle admet des solutions si et seulement si $\text{pgcd}(a\,;b) \mid c$. On trouve une solution particulière (par Bézout), puis **toutes** les solutions en ajoutant les multiples de $\left(\frac{b}{d}\,;-\frac{a}{d}\right)$ où $d = \text{pgcd}(a\,;b)$.
— Relation utile : $\text{pgcd}(a\,;b) \times \text{ppcm}(a\,;b) = ab$ (pour a, b positifs).

Correction de l'exercice 1 – Algorithme d'Euclide

On effectue des divisions euclidiennes successives.

— $1\,071 = 462 \times 2 + 147$;
— $462 = 147 \times 3 + 21$;
— $147 = 21 \times 7 + 0$.
— Le dernier reste non nul est 21, donc $\text{pgcd}(1\,071\,;462) = 21$.
— Contrôle : $1\,071 = 21 \times 51$ et $462 = 21 \times 22$; de plus $\text{pgcd}(51\,;22) = 1$. Correct.

Réponse. $\text{pgcd}(1\,071\,;462) = 21$.

Correction de l'exercice 2 – PGCD et nombres premiers entre eux

a) $84 = 35 \times 2 + 14$; $35 = 14 \times 2 + 7$; $14 = 7 \times 2 + 0$.

— Donc $\text{pgcd}(84\,;35) = 7$.

b) $60 = 17 \times 3 + 9$; $17 = 9 \times 1 + 8$; $9 = 8 \times 1 + 1$; $8 = 1 \times 8 + 0$.

— Le dernier reste non nul est 1 : $\text{pgcd}(17\,;60) = 1$, donc 17 et 60 **sont premiers entre eux**.
— Autre argument pour b) : 17 est premier et ne divise pas 60.

Réponse. a) 7 · b) oui, leur PGCD vaut 1.

Correction de l'exercice 3 – Remonter l'algorithme (Bézout)

On **remonte** l'algorithme d'Euclide effectué précédemment.

— Les divisions étaient : $60 = 17 \times 3 + 9$, $17 = 9 + 8$, $9 = 8 + 1$.
— On isole les restes en partant de la fin :
— $1 = 9 - 8$;
— or $8 = 17 - 9$, donc $1 = 9 - (17 - 9) = 2 \times 9 - 17$;
— or $9 = 60 - 3 \times 17$, donc $1 = 2(60 - 3 \times 17) - 17 = 2 \times 60 - 7 \times 17$.

$$17 \times (-7) + 60 \times 2 = 1$$

— Donc $u = -7$ et $v = 2$.
— Vérification : $-119 + 120 = 1$. Correct.

Réponse. $u = -7$ et $v = 2$.

Correction de l’exercice 4 – Théorème de Bézout

a) **Théorème de Bézout** : deux entiers a et b sont premiers entre eux si et seulement s’il existe des entiers u et v tels que $au + bv = 1$.

b) $\text{pgcd}(12\,;18) = 6 \neq 1$: ils ne sont **pas** premiers entre eux.

— Il est donc **impossible** de trouver u, v avec $12u + 18v = 1$.
— Justification directe : $12u + 18v = 6(2u + 3v)$ est toujours un multiple de 6, et 1 n’en est pas un.
— En revanche, $12u + 18v = 6$ est possible : par exemple $u = -1$ et $v = 1$.

Réponse. b) Non (pgcd = 6) ; l’équation $12u + 18v = 1$ n’a pas de solution.

Correction de l’exercice 5 – Théorème de Gauss

a) On sait que $7 \mid 5n$.

— Or $\text{pgcd}(7\,;5) = 1$ (7 est premier et ne divise pas 5).
— D’après le **théorème de Gauss**, comme 7 divise le produit $5 \times n$ et que 7 est premier avec 5, alors $7 \mid n$.

b) C’est bien le théorème de **Gauss** : si $a \mid bc$ et $\text{pgcd}(a\,;b) = 1$, alors $a \mid c$.

— **Attention** : sans l’hypothèse de primalité entre eux, la conclusion tombe. Par exemple $6 \mid 4 \times 3$ mais $6 \nmid 3$.

Réponse. a) $7 \mid n$ · b) le théorème de Gauss.

Correction de l’exercice 6 – PGCD et PPCM

a) Algorithme d’Euclide : $60 = 36 + 24$; $36 = 24 + 12$; $24 = 12 \times 2 + 0$.

— Donc $\text{pgcd}(36\,;60) = 12$.

b) Relation du cours : $\text{pgcd} \times \text{ppcm} = ab$.

$$\text{ppcm}(36\,;60) = \frac{36 \times 60}{12} = \frac{2\,160}{12} = 180$$

— Contrôle : $180 = 36 \times 5 = 60 \times 3$: c’est bien un multiple commun, et le plus petit.

Réponse. a) 12 · b) 180.

Correction de l’exercice 7 – Condition d’existence d’une solution

Critère du cours : $ax + by = c$ a des solutions si et seulement si $\text{pgcd}(a\,;b) \mid c$.

a) $\text{pgcd}(6\,;9) = 3$, et $3 \mid 21$: il y a des solutions.
b) $3 \nmid 20$: il n’y a **aucune** solution. (En effet $6x + 9y$ est toujours multiple de 3.)

c) $\text{pgcd}(14\,;21) = 7$, et $7 \mid 7$: il y a des solutions (par exemple $x = -1$, $y = 1$).

Réponse. a) oui · b) non · c) oui.

Correction de l'exercice 8 – Solution particulière

— Pour $5x + 3y = 1$: on cherche par tâtonnement (ou par Bézout).
$5 \times (-1) + 3 \times 2 = -5 + 6 = 1$.
— Donc $(x_0\,; y_0) = (-1\,; 2)$.
— Pour $5x + 3y = 7$: on **multiplie** la solution précédente par 7.
— $5 \times (-7) + 3 \times 14 = -35 + 42 = 7$, donc $(-7\,; 14)$ est solution.
— **Méthode générale** : on résout d'abord avec le second membre 1 (possible car $\text{pgcd}(5\,;3) = 1$), puis on multiplie par le second membre voulu.

Réponse. $(-1\,; 2)$ puis $(-7\,; 14)$.

Correction de l'exercice 9 – Solution générale

Étape 1 : solution particulière. On a vu que $(-7\,; 14)$ convient.

Étape 2 : différence. Si $(x\,; y)$ est une autre solution, alors

— $5x + 3y = 7$ et $5 \times (-7) + 3 \times 14 = 7$; en soustrayant : $5(x + 7) + 3(y - 14) = 0$.
— Donc $5(x + 7) = -3(y - 14)$.
— $5 \mid 3(y - 14)$ et $\text{pgcd}(5\,;3) = 1$, donc d'après **Gauss** $5 \mid (y - 14)$: il existe $k \in \mathbb{Z}$ tel que $y = 14 + 5k$.
— En reportant : $5(x + 7) = -15k$, donc $x = -7 - 3k$.

Conclusion : les solutions sont les couples

$$(x\,; y) = (-7 - 3k\,;\, 14 + 5k) \qquad k \in \mathbb{Z}$$

— Contrôle pour $k = -2$: $x = -1$, $y = 4$, et $5 \times (-1) + 3 \times 4 = 7$. Correct.

Réponse. $(x\,; y) = (-7 - 3k\,; 14 + 5k)$, $k \in \mathbb{Z}$.

Correction de l'exercice 10 – Équation avec PGCD non trivial

— $\text{pgcd}(6\,;9) = 3$ et $3 \mid 21$: il y a des solutions.
— On **simplifie** d'abord par 3 : l'équation devient $2x + 3y = 7$.
— Solution particulière : $2 \times 2 + 3 \times 1 = 7$, donc $(2\,;1)$.
— Différence : $2(x - 2) + 3(y - 1) = 0$, soit $2(x - 2) = -3(y - 1)$.
— Comme $\text{pgcd}(2\,;3) = 1$, Gauss donne $2 \mid (y - 1)$, donc $y = 1 + 2k$, puis $x = 2 - 3k$.

$$(x\,; y) = (2 - 3k\,;\, 1 + 2k) \qquad k \in \mathbb{Z}$$

— Contrôle pour $k = 1$: $x = -1$, $y = 3$, et $6 \times (-1) + 9 \times 3 = 21$. Correct.

Réponse. $(x\,; y) = (2 - 3k\,; 1 + 2k)$, $k \in \mathbb{Z}$.

Correction de l'exercice 11 – Application : problème de pièces

a) En notant x le nombre de billets de 5 € et y celui de 2 € : $5x + 2y = 43$.

b) $\text{pgcd}(5\,;2) = 1$: il y a des solutions.

— Solution particulière : $5 \times 1 + 2 \times 19 = 43$, donc $(1\,;19)$.
— Solution générale : $5(x - 1) = -2(y - 19)$, donc $y = 19 - 5k$ et $x = 1 + 2k$.
— **Contraintes de positivité** : $x \geq 0$ donne $k \geq 0$ (pour k entier) ; $y \geq 0$ donne $19 - 5k \geq 0$, soit $k \leq 3{,}8$, donc $k \leq 3$.
— Les solutions possibles sont donc $k \in \{0\,;1\,;2\,;3\}$:

k	**0**	**1**	**2**	**3**
x (billets de 5 €)	1	3	5	7
y (billets de 2 €)	19	14	9	4

— Contrôle pour $k = 3$: $5 \times 7 + 2 \times 4 = 35 + 8 = 43$ €. Correct.

Réponse. b) $(1\,;19)$, $(3\,;14)$, $(5\,;9)$, $(7\,;4)$.

Correction de l’exercice 12 – Utiliser Gauss pour une divisibilité

— $4 \mid n$ donc $n = 4k$.
— $9 \mid n$ donc $9 \mid 4k$.
— Or $\text{pgcd}(9\,;4) = 1$: d’après le **théorème de Gauss**, $9 \mid k$, donc $k = 9k'$.
— Ainsi $n = 4 \times 9k' = 36k'$: n est divisible par 36.
— **Généralisation** : si $b \mid n$, $c \mid n$ et $\text{pgcd}(b\,;c) = 1$, alors $bc \mid n$.
— **Contre-exemple sans l’hypothèse** : $4 \mid 12$ et $6 \mid 12$, mais $24 \nmid 12$ — car $\text{pgcd}(4\,;6) = 2 \neq 1$.

Réponse. Par Gauss : $9 \mid 4k$ et $\text{pgcd}(9\,;4) = 1$ donc $9 \mid k$, d’où $36 \mid n$.

Correction de l’exercice 13 – Synthèse : PGCD dépendant de n

a) $a - 2b = (2n + 3) - 2(n + 1) = 2n + 3 - 2n - 2 = 1$.

b) On utilise la propriété : tout diviseur commun de a et b divise **toute combinaison linéaire** de a et b.

— Soit $d = \text{pgcd}(a\,;b)$. Alors $d \mid a$ et $d \mid b$, donc $d \mid (a - 2b) = 1$.
— Un diviseur positif de 1 vaut 1 : donc $\text{pgcd}(a\,;b) = 1$.
— **Conclusion** : $2n + 3$ et $n + 1$ sont **premiers entre eux** pour tout entier n.
— Contrôle pour $n = 5$: $a = 13$ et $b = 6$, et $\text{pgcd}(13\,;6) = 1$. Cohérent.

Réponse. a) $a - 2b = 1$ · b) $\text{pgcd}(a\,;b) = 1$ pour tout n.