Leçon d'oral du CAPES de mathématiques

Égalité de Bézout

Table des matières

1 Prérequis et objectifs **1**

2 Notions fondamentales **2**
2.1 Divisibilité et PGCD 2
2.2 Combinaisons linéaires entières 2

3 Énoncé et démonstration de l'identité de Bézout **2**
3.1 Théorème de Bézout 2
3.2 Démonstration par le plus petit élément positif 3
3.3 Caractérisation des combinaisons linéaires 3

4 Corollaires et conséquences **4**
4.1 Caractérisation des entiers premiers entre eux 4
4.2 Lien avec les nombres premiers 4

5 Calcul des coefficients de Bézout **4**
5.1 Algorithme d'Euclide 4
5.2 Exemple détaillé 5
5.3 Forme générale des coefficients 5

6 Applications **6**
6.1 Résolution d'équations diophantiennes linéaires 6
6.2 Résolution de congruences 6
6.3 Lien avec le théorème chinois 7

7 Exercices proposés **7**

8 Éléments de correction de quelques exercices **9**

9 Points à souligner à l'oral **11**

10 Conclusion **11**

11 Références bibliographiques **11**

1 Prérequis et objectifs

Prérequis

La compréhension de cette leçon nécessite de maîtriser :

— la division euclidienne dans $\mathbb{Z}$;

— les notions de divisibilité et de multiple dans $\mathbb{Z}$;

— la définition du plus grand commun diviseur de deux entiers ;

— les propriétés élémentaires des congruences ;

— les opérations sur les entiers relatifs.

La division euclidienne constitue un outil fondamental pour établir l'identité de Bézout et construire un algorithme permettant de calculer explicitement ses coefficients.

Objectifs

À l'issue de cette leçon, on doit être capable de :

— énoncer et démontrer l'identité de Bézout ;

— comprendre le lien entre le PGCD de deux entiers et leurs combinaisons linéaires à coefficients entiers ;

— déterminer des coefficients de Bézout à l'aide de l'algorithme d'Euclide étendu ;

— caractériser les couples d'entiers premiers entre eux ;

— appliquer le théorème à la résolution d'équations diophantiennes linéaires et de congruences ;

— expliquer la portée de l'identité de Bézout dans l'arithmétique des entiers.

2 Notions fondamentales

2.1 Divisibilité et PGCD

Définition 2.1. Soient $a, b \in \mathbb{Z}$. Un entier d est un diviseur commun de a et de b si $d \mid a$ et $d \mid b$.

Lorsque a et b ne sont pas tous deux nuls, leur plus grand commun diviseur, noté $\mathrm{PGCD}(a, b)$, est l'unique entier naturel $d > 0$ tel que :

— $d \mid a$ et $d \mid b$;

— tout diviseur commun de a et b divise d.

On adopte la convention $\mathrm{PGCD}(0, 0) = 0$.

Définition 2.2. Deux entiers a et b sont dits premiers entre eux lorsque $\mathrm{PGCD}(a, b) = 1$.

2.2 Combinaisons linéaires entières

Définition 2.3. Une combinaison linéaire entière de deux entiers a et b est un entier de la forme

$$au + bv, \qquad (u, v) \in \mathbb{Z}^2.$$

La question centrale est la suivante : peut-on exprimer le PGCD de deux entiers comme une combinaison linéaire de ces entiers ?

La réponse est affirmative : c'est le contenu de l'identité de Bézout.

3 Énoncé et démonstration de l'identité de Bézout

3.1 Théorème de Bézout

Théorème 3.1 (Identité de Bézout)**.** *Soient $a, b \in \mathbb{Z}$, non tous deux nuls, et soit $d = \mathrm{PGCD}(a, b)$. Il existe deux entiers $u, v \in \mathbb{Z}$ tels que*

$$\boxed{au + bv = d.}$$

Les entiers u et v sont appelés coefficients de Bézout de a et b.

3.2 Démonstration par le plus petit élément positif

Considérons l'ensemble

$$E = \{au + bv \mid (u, v) \in \mathbb{Z}^2,\ au + bv > 0\}.$$

Cet ensemble est non vide puisque a et b ne sont pas tous deux nuls : si $a \neq 0$, l'entier $|a|$ appartient à E ; sinon, $|b|$ appartient à E.

D'après le principe de bon ordre, E possède un plus petit élément positif, noté m. Il existe donc $u_0, v_0 \in \mathbb{Z}$ tels que

$$m = au_0 + bv_0.$$

Effectuons la division euclidienne de a par m :

$$a = qm + r, \qquad 0 \leq r < m.$$

Comme $m = au_0 + bv_0$, on obtient

$$r = a - qm = a(1 - qu_0) + b(-qv_0).$$

Ainsi, r est une combinaison linéaire entière de a et de b.

Si $r > 0$, alors $r \in E$ et $r < m$, ce qui contredit la minimalité de m. Par conséquent, $r = 0$ et donc $m \mid a$.

En procédant de même avec b, on obtient $m \mid b$.

Ainsi, m est un diviseur commun positif de a et de b, donc

$$m \leq \mathrm{PGCD}(a, b) = d.$$

Réciproquement, puisque d divise a et b, il divise toute combinaison linéaire entière de a et de b, en particulier m. Comme $d > 0$ et $m > 0$, on a $d \leq m$.

Il en résulte que $m = d$. Par construction, il existe donc $u_0, v_0 \in \mathbb{Z}$ tels que

$$au_0 + bv_0 = d.$$

L'identité de Bézout est démontrée.

3.3 Caractérisation des combinaisons linéaires

Proposition 3.2. *Soient $a, b \in \mathbb{Z}$, non tous deux nuls, et $d = \mathrm{PGCD}(a, b)$. Alors*

$$\{au + bv \mid u, v \in \mathbb{Z}\} = d\mathbb{Z}.$$

Démonstration. Toute combinaison linéaire $au + bv$ est divisible par d, puisque d divise a et b. Ainsi, l'ensemble considéré est inclus dans $d\mathbb{Z}$.

Réciproquement, d'après l'identité de Bézout, il existe $u_0, v_0 \in \mathbb{Z}$ tels que $au_0 + bv_0 = d$. Pour tout $k \in \mathbb{Z}$,

$$kd = a(ku_0) + b(kv_0).$$

Tout multiple de d est donc une combinaison linéaire entière de a et de b. D'où l'égalité. □

Remarque 3.3. Cette proposition donne une caractérisation particulièrement utile : les combinaisons linéaires entières de a et b sont exactement les multiples de leur PGCD.

4 Corollaires et conséquences

4.1 Caractérisation des entiers premiers entre eux

Corollaire 4.1. *Deux entiers a et b, non tous deux nuls, sont premiers entre eux si et seulement s'il existe $u, v \in \mathbb{Z}$ tels que*

$$au + bv = 1.$$

Démonstration. Si $\mathrm{PGCD}(a, b) = 1$, l'identité de Bézout donne immédiatement le résultat.

Réciproquement, si $au + bv = 1$, tout diviseur commun de a et b divise 1. Le seul diviseur positif commun est donc 1. □

Corollaire 4.2. *Si a et b sont premiers entre eux et si $a \mid bc$, alors $a \mid c$.*

Démonstration. Puisque $\mathrm{PGCD}(a, b) = 1$, il existe $u, v \in \mathbb{Z}$ tels que

$$au + bv = 1.$$

En multipliant par c, on obtient

$$auc + bvc = c.$$

Or a divise auc et, par hypothèse, a divise bc, donc a divise bvc. Par conséquent, $a \mid c$. □

Corollaire 4.3. *Si a et b sont premiers entre eux et divisent un entier n, alors leur produit ab divise n.*

Démonstration. Écrivons $n = ak$. Puisque $b \mid n = ak$ et que $\mathrm{PGCD}(a, b) = 1$, le corollaire précédent donne $b \mid k$. Il existe donc $\ell \in \mathbb{Z}$ tel que $k = b\ell$, d'où $n = ab\ell$. □

4.2 Lien avec les nombres premiers

Proposition 4.4. *Si p est un nombre premier et si $p \nmid a$, alors*

$$\mathrm{PGCD}(p, a) = 1.$$

Par conséquent, si $p \mid ab$, alors $p \mid a$ ou $p \mid b$.

Démonstration. Les seuls diviseurs positifs de p sont 1 et p. Comme p ne divise pas a, le PGCD de p et a vaut 1.

Si $p \mid ab$ et $p \nmid a$, alors $\mathrm{PGCD}(p, a) = 1$. Le corollaire précédent implique $p \mid b$. □

Remarque 4.5. Ce résultat est le lemme d'Euclide. Il intervient notamment dans la démonstration de l'unicité de la décomposition d'un entier naturel supérieur à 1 en produit de facteurs premiers.

5 Calcul des coefficients de Bézout

5.1 Algorithme d'Euclide

L'algorithme d'Euclide repose sur la propriété suivante.

Proposition 5.1. *Pour $a, b \in \mathbb{Z}$, avec $b \neq 0$,*

$$\mathrm{PGCD}(a, b) = \mathrm{PGCD}(b, r),$$

où r est le reste de la division euclidienne de a par b.

Démonstration. Écrivons $a = bq + r$. Tout diviseur commun de a et b divise $r = a - bq$. Réciproquement, tout diviseur commun de b et r divise $a = bq + r$. Les deux couples ont donc les mêmes diviseurs communs. □

5.2 Exemple détaillé

Déterminons le PGCD de 252 et 198, puis des coefficients de Bézout.
Les divisions euclidiennes successives donnent :

$$\begin{aligned} 252 &= 1 \times 198 + 54, \\ 198 &= 3 \times 54 + 36, \\ 54 &= 1 \times 36 + 18, \\ 36 &= 2 \times 18 + 0. \end{aligned}$$

Le dernier reste non nul est 18. Ainsi,

$$\mathrm{PGCD}(252, 198) = 18.$$

Remontons les égalités pour exprimer 18 comme combinaison linéaire de 252 et de 198 :

$$\begin{aligned} 18 &= 54 - 36 \\ &= 54 - (198 - 3 \times 54) \\ &= 4 \times 54 - 198 \\ &= 4(252 - 198) - 198 \\ &= 4 \times 252 - 5 \times 198. \end{aligned}$$

On obtient donc

$$\boxed{252 \times 4 + 198 \times (-5) = 18.}$$

Un couple de coefficients de Bézout est $(4, -5)$.

Remarque 5.2. Les coefficients de Bézout ne sont généralement pas uniques. L'algorithme d'Euclide étendu permet d'en calculer un couple particulier.

5.3 Forme générale des coefficients

Proposition 5.3. *Soient $a, b \in \mathbb{Z}$ non tous deux nuls, $d = \mathrm{PGCD}(a, b)$ et $(u_0, v_0) \in \mathbb{Z}^2$ une solution de*

$$au + bv = d.$$

Si a et b sont tous deux non nuls, toutes les solutions sont données par

$$\boxed{u = u_0 + k\frac{b}{d}, \qquad v = v_0 - k\frac{a}{d}, \qquad k \in \mathbb{Z}.}$$

Démonstration. Si (u, v) est une autre solution, alors

$$a(u - u_0) + b(v - v_0) = 0.$$

En posant $a' = a/d$ et $b' = b/d$, on obtient

$$a'(u - u_0) = -b'(v - v_0).$$

Les entiers a' et b' sont premiers entre eux. Il en résulte que b' divise $u - u_0$ et que a' divise $v - v_0$. Il existe donc $k \in \mathbb{Z}$ tel que

$$u - u_0 = kb', \qquad v - v_0 = -ka'.$$

La réciproque se vérifie par substitution. □

6 Applications

6.1 Résolution d'équations diophantiennes linéaires

On considère l'équation

$$ax + by = c, \qquad (x, y) \in \mathbb{Z}^2.$$

Théorème 6.1. *Si a et b ne sont pas tous deux nuls, l'équation*

$$ax + by = c$$

admet une solution entière si et seulement si

$$\mathrm{PGCD}(a, b) \mid c.$$

Démonstration. Posons $d = \mathrm{PGCD}(a, b)$.

Si une solution existe, alors d divise $ax + by = c$.

Réciproquement, supposons $d \mid c$. Il existe $k \in \mathbb{Z}$ tel que $c = kd$. Par Bézout, on peut écrire $d = au_0 + bv_0$. Ainsi,

$$c = a(ku_0) + b(kv_0),$$

ce qui fournit une solution entière. □

Exemple 6.2. Résolvons dans $\mathbb{Z}^2$ l'équation

$$15x + 21y = 6.$$

Comme $\mathrm{PGCD}(15, 21) = 3$ et $3 \mid 6$, il existe des solutions entières.

L'algorithme d'Euclide donne

$$21 = 15 + 6, \qquad 15 = 2 \times 6 + 3.$$

Ainsi,

$$3 = 15 - 2(21 - 15) = 3 \times 15 - 2 \times 21.$$

En multipliant par 2, on obtient

$$6 = 6 \times 15 - 4 \times 21.$$

Une solution particulière est donc $(x_0, y_0) = (6, -4)$.

La formule générale donne

$$\boxed{x = 6 + 7k, \qquad y = -4 - 5k, \qquad k \in \mathbb{Z}.}$$

6.2 Résolution de congruences

Proposition 6.3. *Soient $a, n \in \mathbb{Z}$ avec $n > 0$. La congruence*

$$ax \equiv b \pmod{n}$$

admet une solution entière si et seulement si

$$\mathrm{PGCD}(a, n) \mid b.$$

Lorsque $\mathrm{PGCD}(a, n) = 1$, la classe de a possède un inverse multiplicatif modulo n.

Démonstration. La congruence équivaut à l'existence de $k \in \mathbb{Z}$ tel que

$$ax - kn = b.$$

C'est une équation diophantienne linéaire, dont le critère de résolubilité est précisément la divisibilité de b par $\mathrm{PGCD}(a, n)$.

Si $\mathrm{PGCD}(a, n) = 1$, Bézout fournit $u, v \in \mathbb{Z}$ tels que

$$au + nv = 1.$$

En réduisant modulo n, on obtient

$$au \equiv 1 \pmod{n}.$$

La classe de u est donc l'inverse de la classe de a. □

Exemple 6.4. Résolvons

$$7x \equiv 3 \pmod{20}.$$

Comme

$$3 \times 7 - 1 \times 20 = 1,$$

l'inverse de 7 modulo 20 est 3. En multipliant la congruence par 3, on obtient

$$x \equiv 9 \pmod{20}.$$

Les solutions sont les entiers de la forme

$$\boxed{x = 9 + 20k, \qquad k \in \mathbb{Z}.}$$

6.3 Lien avec le théorème chinois

L'identité de Bézout joue un rôle essentiel dans le théorème chinois des restes.

Théorème 6.5 (Théorème chinois des restes, cas de deux modules)**.** *Soient $m, n \geq 1$ deux entiers premiers entre eux. Pour tous $a, b \in \mathbb{Z}$, le système*

$$\begin{cases} x \equiv a \pmod{m}, \\ x \equiv b \pmod{n} \end{cases}$$

admet une solution unique modulo mn.

Remarque 6.6. L'identité de Bézout permet notamment de construire explicitement des solutions de ce système. Elle intervient également dans l'arithmétique modulaire et dans certains procédés cryptographiques.

7 Exercices proposés

Les exercices suivants permettent de vérifier la maîtrise des résultats et de préparer des prolongements possibles à l'oral.

Exercice 1 – Calcul du PGCD et coefficients de Bézout

Calculer $\mathrm{PGCD}(414, 276)$ à l'aide de l'algorithme d'Euclide. Déterminer ensuite deux coefficients de Bézout $u, v \in \mathbb{Z}$ tels que

$$414u + 276v = \mathrm{PGCD}(414, 276).$$

Indication : effectuer les divisions euclidiennes successives, puis remonter les égalités.

Exercice 2 – Caractérisation des entiers premiers entre eux

Démontrer que, pour tout $n \in \mathbb{N}$,

$$\mathrm{PGCD}(n, n+1) = 1.$$

En déduire qu'il existe des entiers u, v tels que

$$un + v(n+1) = 1.$$

Déterminer explicitement un tel couple.

Exercice 3 – Équation diophantienne

Résoudre dans $\mathbb{Z}^2$ l'équation

$$35x + 22y = 1.$$

Déterminer ensuite toutes les solutions de

$$35x + 22y = 12.$$

Exercice 4 – Critère de divisibilité

Soient $a, b, c \in \mathbb{Z}$, avec a et b non tous deux nuls. Démontrer que l'équation

$$ax + by = c$$

admet une solution dans $\mathbb{Z}^2$ si et seulement si $\mathrm{PGCD}(a, b) \mid c$.

Appliquer le résultat à l'équation

$$18x + 30y = 7.$$

Exercice 5 – Inverse modulo un entier

Déterminer l'inverse de 17 modulo 43, puis résoudre

$$17x \equiv 5 \pmod{43}.$$

Indication : utiliser l'algorithme d'Euclide étendu.

Exercice 6 – Lemme d'Euclide

Soient $a, b, c \in \mathbb{Z}$ tels que $\mathrm{PGCD}(a, b) = 1$. Démontrer que si $a \mid bc$, alors $a \mid c$.

En déduire que si deux entiers premiers entre eux divisent un même entier, leur produit divise cet entier.

Exercice 7 – Identité de Bézout et fractions irréductibles

Soient $a, b \in \mathbb{Z}$ avec $b \neq 0$ et $\mathrm{PGCD}(a, b) = 1$. Démontrer que, si $a/b = c/d$ avec $c, d \in \mathbb{Z}$ et $d \neq 0$, alors $b \mid d$.

Préciser les conséquences lorsque les deux fractions sont écrites sous forme irréductible avec des dénominateurs positifs.

Exercice 8 – Théorème chinois des restes

Résoudre le système

$$\begin{cases} x \equiv 2 \pmod{5}, \\ x \equiv 3 \pmod{7}. \end{cases}$$

Utiliser l'identité de Bézout pour justifier l'existence et l'unicité de la solution modulo 35.

Exercice 9 – Approfondissement

Soient $a, b \in \mathbb{Z}$ non tous deux nuls. Montrer que l'ensemble

$$I = \{au + bv \mid u, v \in \mathbb{Z}\}$$

est un sous-groupe additif de $\mathbb{Z}$.

Montrer ensuite que tout sous-groupe additif non nul de $\mathbb{Z}$ est de la forme $d\mathbb{Z}$ pour un unique entier $d > 0$.

Retrouver ainsi l'identité de Bézout.

8 Éléments de correction de quelques exercices

Correction de l'exercice 1

Les divisions euclidiennes sont :

$$\begin{aligned} 414 &= 1 \times 276 + 138, \\ 276 &= 2 \times 138 + 0. \end{aligned}$$

Donc

$$\mathrm{PGCD}(414, 276) = 138.$$

Comme $138 = 414 - 276$, un couple de coefficients de Bézout est

$$\boxed{(u, v) = (1, -1).}$$

Correction de l'exercice 2

Tout diviseur commun de n et $n + 1$ divise leur différence :

$$(n + 1) - n = 1.$$

Ainsi, $\mathrm{PGCD}(n, n + 1) = 1$.

De plus,

$$(-1)n + 1(n + 1) = 1.$$

Un couple de coefficients de Bézout est donc $(-1, 1)$.

Correction de l'exercice 3

L'algorithme d'Euclide donne

$$\begin{aligned} 35 &= 22 + 13, \\ 22 &= 13 + 9, \\ 13 &= 9 + 4, \\ 9 &= 2 \times 4 + 1. \end{aligned}$$

En remontant les égalités :

$$\begin{aligned} 1 &= 9 - 2 \times 4 \\ &= 3 \times 9 - 2 \times 13 \\ &= 3 \times 22 - 5 \times 13 \\ &= 8 \times 22 - 5 \times 35. \end{aligned}$$

Ainsi, une solution de $35x + 22y = 1$ est $(-5, 8)$.

Toutes les solutions de $35x + 22y = 1$ sont

$$x = -5 + 22k, \qquad y = 8 - 35k, \qquad k \in \mathbb{Z}.$$

En multipliant une solution particulière par 12, on obtient une solution de $35x + 22y = 12$, à savoir $(-60, 96)$.

Toutes les solutions de cette seconde équation sont

$$\boxed{x = -60 + 22k, \qquad y = 96 - 35k, \qquad k \in \mathbb{Z}.}$$

Correction de l'exercice 4

On a

$$\mathrm{PGCD}(18, 30) = 6.$$

Or 6 ne divise pas 7. L'équation

$$18x + 30y = 7$$

n'admet donc aucune solution entière.

Correction de l'exercice 5

L'algorithme d'Euclide donne

$$\begin{aligned} 43 &= 2 \times 17 + 9, \\ 17 &= 9 + 8, \\ 9 &= 8 + 1. \end{aligned}$$

En remontant :

$$1 = 2 \times 43 - 5 \times 17.$$

Ainsi,

$$17(-5) \equiv 1 \pmod{43}.$$

L'inverse de 17 modulo 43 est donc -5, soit 38 modulo 43.

La congruence

$$17x \equiv 5 \pmod{43}$$

équivaut à

$$x \equiv 5 \times 38 \equiv 18 \pmod{43}.$$

Donc

$$\boxed{x \equiv 18 \pmod{43}.}$$

Correction de l'exercice 8

Le système est

$$\begin{cases} x \equiv 2 \pmod{5}, \\ x \equiv 3 \pmod{7}. \end{cases}$$

Les entiers congrus à 2 modulo 5 sont $2, 7, 12, 17, \ldots$. Parmi eux, $17 \equiv 3 \pmod{7}$.

La solution est donc

$$\boxed{x \equiv 17 \pmod{35}.}$$

Puisque 5 et 7 sont premiers entre eux, le théorème chinois assure l'unicité de cette classe modulo 35.

9 Points à souligner à l'oral

Les éléments suivants méritent d'être explicitement mis en valeur devant le jury :

— **Le rôle de la division euclidienne :** elle permet de calculer le PGCD et de remonter les égalités pour obtenir les coefficients de Bézout.

— **La distinction entre existence et unicité :** le PGCD est unique, mais les coefficients de Bézout ne le sont généralement pas.

— **Le lien entre théorie et algorithme :** le théorème de Bézout possède une preuve théorique et une méthode constructive de calcul.

— **Les applications :** équations diophantiennes, inverses modulo un entier, congruences et théorème chinois.

— **La rigueur des hypothèses :** le couple (a, b) ne doit pas être $(0, 0)$ dans l'énoncé usuel, et le PGCD est pris positif lorsqu'il n'est pas nul.

10 Conclusion

L'identité de Bézout constitue un résultat fondamental de l'arithmétique des entiers. Elle établit que le PGCD de deux entiers non tous deux nuls est une combinaison linéaire entière de ces deux entiers.

Elle fournit une caractérisation des couples d'entiers premiers entre eux et permet de résoudre des équations diophantiennes linéaires. L'algorithme d'Euclide étendu en donne une méthode de calcul effective, qui trouve notamment des applications dans l'arithmétique modulaire.

11 Références bibliographiques

Références

[1] Euclide, *Les Éléments*, livres VII et IX. Référence historique pour la théorie de la divisibilité et des nombres premiers.

[2] G. H. Hardy et E. M. Wright, *An Introduction to the Theory of Numbers*, Oxford University Press. Ouvrage de référence sur l'arithmétique des entiers et les propriétés des nombres premiers.

[3] Michel Demazure, *Cours d'algèbre : primalité, divisibilité, codes*, Cassini. Référence pour l'arithmétique et les structures algébriques.

[4] Xavier Gourdon, *Les maths en tête – Algèbre*, Ellipses. Ouvrage d'exercices et de résultats d'algèbre utile pour approfondir les méthodes de démonstration.

[5] Ministère de l'Éducation nationale, *Programmes de mathématiques du collège et du lycée général et technologique*. Bulletins officiels disponibles sur le site du ministère : https://www.education.gouv.fr/.