Math93.com

TD 2 - Tle Maths Expertes
Arithmétique Partie 2

Les exercices dont l'intitulé est précédé du symbole (c) sont intégralement corrigés en fin de TD.

Table des matières

Partie I. PGCD et nombres premiers entre eux

Exercice 1. (c)

Déterminons les entiers naturels n inférieurs à 450 tels que PGCD$(n, 270) = 45$.

Exercice 2. (c) Avec une suite (ex. 63)

On définit, pour tout entier $n \geqslant 1$, la suite (u_n) par :

$$u_n = \frac{1}{n} \times \text{PGCD}(24, n).$$

La suite (u_n) est-elle convergente ?

Exercice 3. (c) PGCD et propriétés (ex. 64)

Montrer que, pour tout entier naturel n,

$$\text{PGCD}(3n + 4, 4n + 3) = 7 \iff n \equiv 1 \pmod 7.$$

Exercice 4. (c) PGCD et propriétés (ex. 68)

Soient n un entier naturel, $\alpha = 2n + 1$ et $\beta = n + 3$.

1. Montrer que PGCD(α, β) divise 5.
2. Montrer que si $n \equiv 2 \pmod 5$, alors 5 est un diviseur commun à α et β.
3. En déduire que PGCD$(\alpha, \beta) = 5$ si, et seulement si, $n \equiv 2 \pmod 5$.

Exercice 5. Algorithme d'Euclide (c)

Déterminer, avec l'algorithme d'Euclide :

1. le $PGCD$ de 7 548 et 2 574.
2. le $PGCD$ de 9 504 et 7 488.

Exercice 6. (c) (ex. 76)

Un son complexe est composé d'une harmonique A de fréquence 440 hertz, d'une harmonique B de fréquence 520 hertz et d'une harmonique C de fréquence 780 hertz. On admet que la fréquence de ce son est égale au PGCD des fréquences des harmoniques. Quelle est la fréquence de ce son complexe ?

Exercice 7. (c) Une application du théorème

On rappelle la propriété suivante :

Propriété 1

Soient a et b deux entiers relatifs non nuls.

- Soient $d = \text{PGCD}(a, b)$ et a', b' les entiers tels que $a = da'$ et $b = db'$.
  Alors, a' et b' sont premiers entre eux.
- Réciproquement, s'il existe $d \in \mathbb{N}$ et a', b' des entiers premiers entre eux tels que $a = da'$ et $b = db'$, alors d est le PGCD de a et b.

Déterminer l'ensemble des couples $(a, b) \in \mathbb{N}^2$ tels que :

$$\begin{cases} ab = 300, \\ \text{PGCD}(a, b) = 5. \end{cases}$$

Méthode

- Introduire les entiers a' et b' premiers entre eux tels que :
$$\begin{cases} a = 5a', \\ b = 5b'. \end{cases}$$
- Écrire une équation vérifiée par le produit $a'b'$ et lister les couples d'entiers premiers entre eux vérifiant cette équation.
- En déduire les valeurs possibles pour a et b.

Exercice 8. (c) Sur le même modèle que l'exercice 7

1. Déterminer l'ensemble des couples $(x, y) \in \mathbb{N}^2$ tels que :

$$\begin{cases} xy = 6348, \\ \text{PGCD}(x, y) = 23. \end{cases}$$

2. Déterminer l'ensemble des couples $(a, b) \in \mathbb{N}^2$ tels que :

$$\begin{cases} a + b = 72, \\ \text{PGCD}(a, b) = 9. \end{cases}$$

Partie II. Théorèmes de Bachet-Bézout

Théorème 1 (Bézout, 1730-1883 / Bachet, 1581-1638)

Deux entiers naturels a et b sont premiers entre eux, si et seulement si, il existe deux entiers u et v tels que $au + bv = 1$.

Soit :

$$\boxed{\text{PGCD}\,(a\ ;\ b) = 1 \iff \exists\,(u\ ;\ v) \in \mathbb{Z}^2\ ;\ au + bv = 1}$$

Remarque : C'est le groupe Bourbaki qui attribue, vers 1948, le nom de Bézout à ce théorème, bien que celui-ci ait été énoncé et démontré par le mathématicien français Claude-Gaspard Bachet de Méziriac (1581-1638) dans son ouvrage *Problèmes plaisants et délectables*, publié en 1624. Bézout, quant à lui, établit en 1764 une généralisation de ce théorème aux polynômes dans un mémoire présenté à l'Académie des sciences.

Exercice 9. (c) Pour montrer que des nombre sont premiers entre eux (ex. 83, 45 et 46)

Méthode

Dans ce genre d'exercices, on cherche à écrire une combinaison linéaire des deux expressions qui donne 1.

1. Soit $n \in \mathbb{N}$. Montrer, à l'aide du théorème de Bézout, que :

$$\text{PGCD}(4n + 3, 2n + 1) = 1.$$

2. Soit $n \in \mathbb{N}$. Montrer à l'aide du théorème de Bézout que $5n - 7$ et $2n - 3$ sont premiers entre eux.

Exercice 10. (c) Pour chercher les coefficients de Bezout

1. Soit $a = 86$ et $b = 77$. Déterminer en appliquant l'algorithme d'Euclide un couple $(u\ ;\ v)$ tel que $au + bv = 1$.

Méthode

- On commence par justifier qu'il existe bien un couple d'entiers (u, v) tel que :

$$86u + 77v = 1.$$

- On applique l'algorithme d'Euclide pour connaître tous les restes successifs jusqu'au reste égal à 1.
- Puis, on utilise les divisions euclidiennes obtenues en « remontant » l'algorithme d'Euclide afin de déterminer u et v.

2. Soit $a = 112$ et $b = 17$. Déterminer en appliquant l'algorithme d'Euclide un couple $(u\ ;\ v)$ tel que $au + bv = 1$.

Exercice 11. (c) Inverse modulo 23 ?

Après avoir justifié son existence, déterminer un entier a tel que :

$$30a \equiv 1 \pmod{23}.$$

Partie III. Identité de Bézout et applications

Propriété 2

a et b sont deux entiers relatifs non nuls.
Si d est le PGCD de a et de b, **alors** il existe deux entiers relatifs u et v tels que $au + bv = d$.

Ce que l'on peut écrire :

$$\boxed{a \wedge b = d \Longrightarrow \exists (u\ ;\ v) \in \mathbb{Z}^2\ \ ,\ \ au + bv = d}$$

Exercice 12. (c) Application de Bézout 2

Déterminer le PGCD d de 117 et 198 puis des coefficients de Bézout associés.

Exercice 13. (c) Application de Bézout 3

Déterminer le PGCD d de 84 et 18 puis des coefficients de Bézout associés.

Partie IV. Théorème de Gauss

Théorème 2 (Carl Friedrich Gauss, 1777-1855)

Soit a, b, c des entiers.

Si $\begin{cases} a \text{ divise le produit } bc \\ a \text{ et } b \text{ sont premiers entre eux} \end{cases}$, alors a divise c.

Ce que l'on peut écrire :

$$\begin{cases} a \mid bc \\ a \wedge b = 1 \end{cases} \Longrightarrow a \mid c$$

Remarque : Le mathématicien allemand Carl Friedrich Gauss énonce et prouve ce théorème (sous forme de lemme en fait) en 1801 dans son ouvrage « *Disquisitiones arithmeticae* ».

Exercice 14. (c)

Méthode

1. On applique l'algorithme d'Euclide : le dernier reste non nul est le PGCD cherché.
2. On simplifie l'équation par le PGCD pour obtenir deux nombres premiers entre eux et on utilise alors le théorème de Gauss pour obtenir une expression de X et Y. On vérifie que le couple obtenu est bien solution de l'équation.

1. Déterminer le PGCD de 65 et 91.
2. Résoudre dans $\mathbb{Z}^2$ l'équation :
$$65X = 91Y.$$

Exercice 15. (c) Équation Diophantienne 1

Déterminer les solutions de l'équation (E') : $6u + 11v = 7$.

Exercice 16. (c) Équation Diophantienne 2

Déterminer les solutions de l'équation (E') : $5u + 7v = 8$.

Partie V. Bilan

Exercice 17. D'après bac

À toute lettre de l'alphabet on associe un nombre entier x compris entre 0 et 25 comme indiqué dans le tableau ci-dessous :

Lettre	A	B	C	D	E	F	G	H	I	J	K	L	M
x	0	1	2	3	4	5	6	7	8	9	10	11	12
Lettre	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
x	13	14	15	16	17	18	19	20	21	22	23	24	25

Le « chiffre de RABIN » est un dispositif de cryptage asymétrique inventé en 1979 par l'informaticien Michael Rabin.

Alice veut communiquer de manière sécurisée en utilisant ce cryptosystème. Elle choisit deux nombres premiers distincts p et q. Ce couple de nombres est sa clé privée qu'elle garde secrète.
Elle calcule ensuite $n = p \times q$ et elle choisit un nombre entier naturel B tel que $0 \leqslant B \leqslant n-1$.
Si Bob veut envoyer un message secret à Alice, il le code lettre par lettre.
Le codage d'une lettre représentée par le nombre entier x est le nombre y tel que :

$$y \equiv x(x+B) \ [n] \text{ avec } 0 \leqslant y \leqslant n.$$

Dans tout l'exercice on prend $p = 3,\ q = 11$ donc $n = p \times q = 33$ et $B = 13$.

Partie A : Cryptage

Bob veut envoyer le mot « NO » à Alice.

1. Montrer que Bob code la lettre « N » avec le nombre 8.

2. Déterminer le nombre qui code la lettre « O ».

Partie B : Décryptage

Alice a reçu un message crypté qui commence par le nombre 3.
Pour décoder ce premier nombre, elle doit déterminer le nombre entier x tel que :

$$x(x+13) \equiv 3 \ [33] \text{ avec } 0 \leqslant x < 26.$$

1. Montrer que $x(x+13) \equiv 3 \ [33]$ équivaut à $(x+23)^2 \equiv 4 \ [33]$.

2. 2. a. Montrer que si $(x+23)^2 \equiv 4 \ [33]$ alors le système d'équations $\begin{cases} (x+23)^2 \equiv 4 \ [3] \\ (x+23)^2 \equiv 4 \ [11] \end{cases}$ est vérifié.

2. b. Réciproquement, montrer que si $\begin{cases} (x+23)^2 \equiv 4 \ [3] \\ (x+23)^2 \equiv 4 \ [11] \end{cases}$ alors $(x+23)^2 \equiv 4 \ [33]$.

2. c. En déduire que $x(x+13) \equiv 3 \ [33] \iff \begin{cases} (x+23)^2 \equiv 1 \ [3] \\ (x+23)^2 \equiv 4 \ [11] \end{cases}$

3. 3. a. Déterminer les nombres entiers naturels a tels que $0 \leqslant a < 3$ et $a^2 \equiv 1 \ [3]$.

3. b. Déterminer les nombres entiers naturels b tels que $0 \leqslant b < 11$ et $b^2 \equiv 4 \ [11]$.

4. 4. a. En déduire que $x(x+13) \equiv 3 \ [33]$ équivaut aux quatre systèmes suivants :

$$\begin{cases} x \equiv 2 \ [3] \\ x \equiv 8 \ [11] \end{cases} \text{ ou } \begin{cases} x \equiv 0 \ [3] \\ x \equiv 1 \ [11] \end{cases} \text{ ou } \begin{cases} x \equiv 2 \ [3] \\ x \equiv 1 \ [11] \end{cases} \text{ ou } \begin{cases} x \equiv 0 \ [3] \\ x \equiv 8 \ [11] \end{cases}$$

4. b. On admet que chacun de ces systèmes admet une unique solution entière x telle que $0 \leqslant x < 33$.

Déterminer, sans justification, chacune de ces solutions.

5. Compléter l'algorithme en **Annexe** pour qu'il affiche les quatre solutions trouvées dans la question précédente.

6. Alice peut-elle connaître la première lettre du message envoyé par Bob ?

Le « chiffre de RABIN » est-il utilisable pour décoder un message lettre par lettre ?

Fin du TD

Partie VI. Corrections

Correction de l'exercice 1

Déterminons les entiers naturels n inférieurs à 450 tels que $\text{PGCD}(n, 270) = 45$.

Corrigé

On sait que 45 divise n, donc il existe un entier $m \in \mathbb{N}$ tel que :

$$n = 45m.$$

De plus, puisque $n \leqslant 450$, on en déduit que :

$$m \leqslant \frac{450}{45} = 10.$$

Par ailleurs, on utilise la propriété du PGCD :

$$\text{PGCD}(n, 270) = \text{PGCD}(45m, 45 \times 6) = 45 \times \text{PGCD}(m, 6).$$

Or, par hypothèse, $\text{PGCD}(n, 270) = 45$, donc :

$$45 \times \text{PGCD}(m, 6) = 45.$$

On en conclut que :

$$\text{PGCD}(m, 6) = 1.$$

Les entiers m inférieurs ou égaux à 10 et premiers avec 6 sont :

$$m \in \{1, 5, 7\}.$$

Finalement, en remplaçant m dans l'expression de n, on obtient :

$$n \in \{45, 225, 315\}.$$

Correction de l'exercice 2

On définit, pour tout entier $n \geqslant 1$, la suite (u_n) par :

$$u_n = \frac{1}{n} \times \text{PGCD}(24, n).$$

La suite (u_n) est-elle convergente ?

Corrigé

Pour tout $n \in \mathbb{N}$, on a :

$$0 \leqslant \text{PGCD}(24, n) \leqslant 24.$$

Ainsi, pour tout $n \geqslant 1$, il vient :

$$0 \leqslant \frac{1}{n}\text{PGCD}(24, n) \leqslant \frac{24}{n}.$$

Or, on sait que $\frac{24}{n}$ tend vers 0 lorsque $n \to +\infty$. Par le théorème d'encadrement, on en déduit que la suite (u_n) converge vers 0.

Correction de l'exercice 3

Montrer que, pour tout entier naturel n,

$$\text{PGCD}(3n+4, 4n+3) = 7 \iff n \equiv 1 \pmod 7.$$

Corrigé

Pour tout $n \in \mathbb{N}$, on a par combinaisons linéaires :

$$\text{PGCD}(3n+4, 4n+3) = \text{PGCD}(3n+4, n-1) = \text{PGCD}(7, n-1).$$

Or,

$$\text{PGCD}(7, n-1) = 7 \text{ si } 7 \text{ divise } n-1$$

Autrement dit,

$$\text{PGCD}(3n+4, 4n+3) = 7 \iff n \equiv 1 \pmod 7.$$

Correction de l'exercice 4

Soient n un entier naturel, $\alpha = 2n+1$ et $\beta = n+3$.

1. Montrer que PGCD(α, β) divise 5.

Corrigé

On a :

$$\text{PGCD}(2n+1, n+3) = \text{PGCD}(-5, n+3) = \text{PGCD}(5, n+3).$$

Donc, PGCD$(2n+1, n+3)$ est un diviseur de 5.

2. Montrer que si $n \equiv 2 \pmod 5$, alors 5 est un diviseur commun à α et β.

Corrigé

Si $n \equiv 2 \pmod 5$, alors :

$$2n+1 \equiv 2 \times 2 + 1 \equiv 0 \pmod 5.$$

Donc, $\alpha \equiv 0 \pmod 5$, c'est-à-dire que 5 divise α.

De même, si $n \equiv 2 \pmod 5$, alors :

$$n+3 \equiv 2+3 \equiv 0 \pmod 5.$$

Donc, $\beta \equiv 0 \pmod 5$, c'est-à-dire que 5 divise β.

En conclusion, 5 est un diviseur commun à α et β.

3. En déduire que PGCD$(\alpha, \beta) = 5$ si, et seulement si, $n \equiv 2 \pmod 5$.

Corrigé

On a montré que si $n \equiv 2 \pmod 5$, alors 5 divise α et β, donc 5 divise leur PGCD.

De plus, d'après la première question, PGCD$(2n+1, n+3)$ divise 5.

D'où :

$$\text{PGCD}(2n+1, n+3) = 5.$$

Réciproquement, si PGCD$(2n+1, n+3) = 5$, alors 5 divise $n+3$, donc :

$$n \equiv -3 \pmod 5.$$

Or, $-3 \equiv 2 \pmod 5$, donc $n \equiv 2 \pmod 5$.

D'où l'équivalence.

Correction de l'exercice 5

Déterminer, avec l'algorithme d'Euclide :

1. le $PGCD$ de 7 548 et 2 574.
2. le $PGCD$ de 9 504 et 7 488.

Correction

Calculons par l'algorithme d'EUCLIDE le PGCD des nombres 7548 et 2574.
Cet algorithme porte le nom du mathématicien grec *Euclide de Samos* (vers 300 av. J.-C.), auteur des « *Eléments* ».
Il est basé sur la propriété suivante :

Propriété 3

Pour a, b entiers tels que $a \geqslant b > 0$ et r le reste de la division euclidienne de a par b :

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

Par divisions euclidiennes successives on obtient :

$$\begin{aligned}
7548 &= 2574 \times 2 + 2400\\
2574 &= 2400 \times 1 + 174\\
2400 &= 174 \times 13 + 138\\
174 &= 138 \times 1 + 36\\
138 &= 36 \times 3 + 30\\
36 &= 30 \times 1 + 6\\
30 &= 6 \times 5 + 0
\end{aligned}$$

Le PGCD des nombres 7548 et 2574 est le dernier reste non nul du procédé, c'est-dire 6.

$$\boxed{\text{PGCD}\,(7548\,;\,2574) = 6}$$

On peut vérifier que 6 divise bien 7548 et 2574 :

$$7548 \div 6 = 1258 \text{ et } 2574 \div 6 = 429$$

Correction

Calculons par l'algorithme d'EUCLIDE le PGCD des nombres 9504 et 7488.
Cet algorithme porte le nom du mathématicien grec *Euclide de Samos* (vers 300 av. J.-C.), auteur des « *Eléments* ».
Il est basé sur la propriété suivante :

Propriété 4

Pour a, b entiers tels que $a \geqslant b > 0$ et r le reste de la division euclidienne de a par b :

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

Par divisions euclidiennes successives on obtient :
Le PGCD des nombres 9504 et 7488 est le dernier reste non nul du procédé, c'est-dire 288.

$$\boxed{\text{PGCD}\,(9504\,;\,7488) = 288}$$

On peut vérifier que 288 divise bien 9504 et 7488 :

$$9504 \div 288 = 33 \text{ et } 7488 \div 288 = 26$$

Correction de l'exercice 6

Un son complexe est composé d'une harmonique A de fréquence 440 hertz, d'une harmonique B de fréquence 520 hertz et d'une harmonique C de fréquence 780 hertz. On admet que la fréquence de ce son est égale au PGCD des fréquences des harmoniques. Quelle est la fréquence de ce son complexe ?

Correction

On cherche le PGCD de 440, 520 et 780.

$$\text{PGCD}(440, 520) = 10 \times \text{PGCD}(44, 52) = 40 \times \text{PGCD}(11, 13) = 40$$

car 11 et 13 sont premiers entre eux.
De plus,

$$\text{PGCD}(440, 780) = 10 \times \text{PGCD}(44, 78) = 20 \times \text{PGCD}(22, 39) = 20$$

car 22 et 39 sont premiers entre eux.
On en déduit que le PGCD de 440, 520 et 780 est 20. Le son complexe considéré a donc une fréquence de 20 Hz.

Correction de l'exercice 7

Propriété 5

Soient a et b deux entiers relatifs non nuls.

- Soient $d = \text{PGCD}(a, b)$ et a', b' les entiers tels que $a = da'$ et $b = db'$.
  Alors, a' et b' sont premiers entre eux.
- Réciproquement, s'il existe $d \in \mathbb{N}$ et a', b' des entiers premiers entre eux tels que $a = da'$ et $b = db'$, alors d est le PGCD de a et b.

Déterminer l'ensemble des couples $(a, b) \in \mathbb{N}^2$ tels que :

$$\begin{cases} ab = 300, \\ \text{PGCD}(a, b) = 5. \end{cases}$$

Méthode

- Introduire les entiers a' et b' premiers entre eux tels que :
$$\begin{cases} a = 5a', \\ b = 5b'. \end{cases}$$
- Écrire une équation vérifiée par le produit $a'b'$ et lister les couples d'entiers premiers entre eux vérifiant cette équation.
- En déduire les valeurs possibles pour a et b.

Corrigé

- Sens direct : Puisque $\text{PGCD}(a, b) = 5$, il existe deux entiers a' et b' premiers entre eux tels que :
$$\begin{cases} a = 5a', \\ b = 5b'. \end{cases}$$
On a alors :
$$ab = (5a')(5b') = 25a'b'$$
d'où :
$$25a'b' = 300 \iff a'b' = 12.$$
Or, les décompositions de 12 en produits de deux nombres premiers entre eux sont :
$$12 = 1 \times 12 = 2 \times 6 = 3 \times 4.$$
Comme a' et b' doivent être premiers entre eux, les couples possibles sont :
$$(1, 12), (12, 1), (3, 4), (4, 3).$$
Ce qui donne pour (a, b) les couples :
$$(5, 60), (60, 5), (15, 20), (20, 15).$$
- Réciproquement, chacun de ces couples est solution du système.

Correction de l'exercice 8

1. Déterminer l'ensemble des couples $(x, y) \in \mathbb{N}^2$ tels que :

$$\begin{cases} xy = 6348, \\ \text{PGCD}(x, y) = 23. \end{cases}$$

Corrigé

Par hypothèse, $\text{PGCD}(x, y) = 23$, donc 23 divise à la fois x et y. Soient u et v les entiers naturels tels que :

$$x = 23u, \quad y = 23v.$$

Ainsi, en remplaçant dans l'équation du produit :

$$xy = 6348 \Rightarrow (23u)(23v) = 6348 \Rightarrow uv = 12.$$

On obtient alors les décompositions suivantes :

$$\begin{cases} u = 1, & v = 12, \\ u = 3, & v = 4, \\ u = 2, & v = 6, \end{cases}$$

ou inversement (on peut échanger les valeurs de u et v).
Or, (u, v) doit vérifier la propriété suivante :

$$\text{PGCD}(x, y) = 23\text{PGCD}(u, v),$$

ce qui implique que $\text{PGCD}(u, v) = 1$.
Seuls les deux premiers cas sont donc possibles. On en déduit que :

$$(x, y) \in \{(23, 276), (69, 92), (276, 23), (92, 69)\}.$$

Réciproquement, on vérifie que ces couples sont bien solutions du problème.

2. Déterminer l'ensemble des couples $(a, b) \in \mathbb{N}^2$ tels que :

$$\begin{cases} a + b = 72, \\ \text{PGCD}(a, b) = 9. \end{cases}$$

Corrigé

Soit $(a, b) \in \mathbb{N}^2$ tel que :

$$a + b = 72 \quad \text{et} \quad \text{PGCD}(a, b) = 9.$$

Soient c et d les entiers naturels tels que :

$$a = 9c, \quad b = 9d.$$

On peut donc écrire :

$$9c + 9d = 72,$$

d'où :

$$c + d = 8 \quad \text{et} \quad \text{PGCD}(c, d) = 1.$$

On en déduit que :

$$(c, d) \in \{(1, 7), (3, 5), (7, 1), (5, 3)\},$$

d'où :

$$(a, b) \in \{(9, 63), (27, 45), (63, 9), (45, 27)\}.$$

- Réciproquement, on vérifie que ces couples sont bien solutions du problème.

Correction de l'exercice 9

Méthode

Dans ce genre d'exercice, on cherche à écrire une combinaison linéaire des deux expressions qui donne 1.

1. Soit $n \in \mathbb{N}$. Montrer, à l'aide du théorème de Bézout, que :

$$\text{PGCD}(4n+3, 2n+1) = 1.$$

Corrigé

On a l'égalité :

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

Il existe donc deux entiers relatifs u et v tels que :

$$u(4n+3) + v(2n+1) = 1.$$

D'après le théorème de Bézout, cela implique que $4n+3$ et $2n+1$ sont premiers entre eux.

2. Soit $n \in \mathbb{N}$. Montrer à l'aide du théorème de Bézout que $5n-7$ et $2n-3$ sont premiers entre eux.

Corrigé

$$2(5n-7) - 5(2n-3) = 1$$

donc, d'après le théorème de Bézout, $5n-7$ et $2n-3$ sont premiers entre eux.

Correction de l'exercice 10

1. Soit $a = 86$ et $b = 77$. Déterminer en appliquant l'algorithme d'Euclide un couple $(u\ ;\ v)$ tel que $au + bv = 1$.

Correction

Par divisions euclidiennes successives on obtient avec $a = 86$ et $b = 77$:

Division euclidienne	**Reste**	**Egalité avec a et b**
$86 = 77 \times 1 + 9$	$9 = 86 - 1 \times 77$	$9 = a - 1\ b$
$77 = 9 \times 8 + 5$	$5 = 77 - 8 \times 9$	$5 = b - 8 \times (a - 1\ b)$ $5 = -8\ a + 9\ b$
$9 = 5 \times 1 + 4$	$4 = 9 - 1 \times 5$	$4 = (1\ a - 1\ b) - 1 \times (-8\ a + 9\ b)$ $4 = 9\ a + (-10)\ b$
$5 = 4 \times 1 + 1$	$1 = 5 - 1 \times 4$	$1 = (-8\ a + 9\ b) - 1 \times (9\ a - 10\ b)$ $1 = -17\ a + 19\ b$

Le PGCD des nombres 86 et 77 est le dernier reste non nul du procédé, c'est-dire 1.
Les nombres 86 et 77 sont donc premiers entre eux et le théore 1 dit de Bézout-Bachet assure donc l'existence de couples $(u\ ;\ v)$ d'entiers relatifs solutions de l'équation :

$$86\ u + 77\ v = 1$$

Pour trouver une solution, il suffisait d'exprimer le reste de la division euclidienne en fonction de a et b pour chaque ligne du procédé. Un couple solution de l'équation $86\ u + 77\ v = 1$ est donc :

$$\boxed{(u = -17\ ;\ v = 19)}$$

2. Soit $a = 112$ et $b = 17$. Déterminer en appliquant l'algorithme d'Euclide un couple $(u\ ;\ v)$ tel que $au + bv = 1$.

Correction

Par divisions euclidiennes successives on obtient avec $a = 112$ et $b = 17$:

Division euclidienne	**Reste**	**Egalité avec a et b**
$112 = 17 \times 6 + 10$	$10 = 112 - 6 \times 17$	$10 = a - 6\ b$
$17 = 10 \times 1 + 7$	$7 = 17 - 1 \times 10$	$7 = b - 1 \times (a - 6\ b)$ $7 = -1\ a + 7\ b$
$10 = 7 \times 1 + 3$	$3 = 10 - 1 \times 7$	$3 = (1\ a - 6\ b) - 1 \times (-1\ a + 7\ b)$ $3 = 2\ a + (-13)\ b$
$7 = 3 \times 2 + 1$	$1 = 7 - 2 \times 3$	$1 = (-1\ a + 7\ b) - 2 \times (2\ a - 13\ b)$ $1 = -5\ a + 33\ b$

Le PGCD des nombres 112 et 17 est le dernier reste non nul du procédé, c'est-dire 1.
Les nombres 112 et 17 sont donc premiers entre eux et le théore 1 dit de Bézout-Bachet assure donc l'existence de couples $(u\ ;\ v)$ d'entiers relatifs solutions de l'équation :

$$112\ u + 17\ v = 1$$

Pour trouver une solution, il suffisait d'exprimer le reste de la division euclidienne en fonction de a et b pour chaque ligne du procédé. Un couple solution de l'équation $112\,u + 17\,v = 1$ est donc :

$$\boxed{(u = -5\ ;\ v = 33)}$$

Correction de l'exercice 11

Après avoir justifié son existence, déterminer un entier a tel que :

$$30a \equiv 1 \pmod{23}.$$

Correction

30 et 23 sont premiers entre eux, donc, d'après le théorème de Bézout, il existe un couple d'entiers relatifs (a, b) tel que :

$$30a + 23b = 1.$$

Ainsi, il existe un entier a tel que :

$$30a \equiv 1 \pmod{23}.$$

L'algorithme d'Euclide et sa remontée permettent d'obtenir :

$$1 = 30 \times 10 - 23 \times 13.$$

On en déduit que $(10, -13)$ est un couple solution et donc que 10 est un inverse de 30 modulo 23 :

$$30 \times 10 \equiv 1 \pmod{23}.$$

Correction de l'exercice 12

Déterminer le PGCD d de 117 et 198 puis des coefficients de Bézout associés.

Correction

1. Le PGCD de 117 et 198 est 9 donc il existe des entiers u et v tels que :

$$117u + 198v = 9$$

2. Pour les déterminer, on peut se ramener à l'équation diophantienne :

$$13u + 22v = 1$$

Par divisions euclidiennes successives on obtient avec $a = 13$ et $b = 22$:

Division euclidienne	**Reste**	**Egalité avec a et b**
$13 = 22 \times 0 + 13$	$13 = 13 - 0 \times 22$	
$22 = 13 \times 1 + 9$	$9 = 22 - 1 \times 13$	$9 = -1\ a + 1\ b$
$13 = 9 \times 1 + 4$	$4 = 13 - 1 \times 9$	$4 = a - 1\ b$
$9 = 4 \times 2 + 1$	$1 = 9 - 2 \times 4$	$1 = (-1\ a + 1\ b) - 2 \times (2\ a - 1\ b)$ $1 = -5\ a + 3\ b$

Le PGCD des nombres 13 et 22 est le dernier reste non nul du procédé, c'est-dire 1.
Les nombres 13 et 22 sont donc premiers entre eux et le théore 1 dit de Bézout-Bachet assure donc l'existence de couples $(u\ ;\ v)$ d'entiers relatifs solutions de l'équation :

$$13\ u + 22\ v = 1$$

Pour trouver une solution, il suffisait d'exprimer le reste de la division euclidienne en fonction de a et b pour chaque ligne du procédé. Un couple solution de l'équation $13\ u + 22\ v = 1$ est donc :

$$\boxed{(u = -5\ ;\ v = 3)}$$

Correction de l'exercice 13

Déterminer le PGCD d de 84 et 18 puis des coefficients de Bézout associés.

Correction

Le PGCD de 84 et 18 est 6, donc il existe des entiers u et v tels que :

$$84u + 18v = 6.$$

Pour les déterminer, on peut se ramener à l'équation diophantienne :

$$14u + 3v = 1,$$

dont une solution est $(-1, 5)$. Vérifions :

$$-84 + 18 \times 5 = -84 + 90 = 6.$$

Correction de l'exercice 14

Méthode

1. On applique l'algorithme d'Euclide : le dernier reste non nul est le PGCD cherché.
2. On simplifie l'équation par le PGCD pour obtenir deux nombres premiers entre eux et on utilise alors le théorème de Gauss pour obtenir une expression de X et Y.
3. On vérifie que le couple obtenu est bien solution de l'équation.

1. Déterminer le PGCD de 65 et 91.
2. Résoudre dans $\mathbb{Z}^2$ l'équation :
$$65X = 91Y.$$

Correction

1. On applique l'algorithme d'Euclide :
$$91 = 65 \times 1 + 26,$$
$$65 = 26 \times 2 + 13,$$
$$26 = 13 \times 2 + 0.$$
Donc, $\text{PGCD}(91, 65) = 13$.

2. En divisant par 13, on obtient :
$$65X = 91Y \quad \Leftrightarrow \quad 5X = 7Y.$$
Or, $5X = 7Y$ implique $7 \mid 5X$, et comme 5 et 7 sont premiers entre eux, d'après le théorème de Gauss, on a :
$$7 \mid X.$$
Ainsi, si (X, Y) est solution de l'équation, alors il existe $k \in \mathbb{Z}$ tel que :
$$X = 7k.$$
En remplaçant dans l'équation :
$$5X = 7Y \quad \Rightarrow \quad 5 \times 7k = 7 \times Y,$$
d'où :
$$Y = 5k.$$
Réciproquement, on vérifie que, pour tout $k \in \mathbb{Z}$, $(7k, 5k)$ est un couple solution :
$$65 \times 7k = 455k \quad \text{et} \quad 91 \times 5k = 455k.$$
Donc, pour tout entier k, $(7k, 5k)$ est un couple solution.
Finalement, l'ensemble des solutions de l'équation est :
$$\{(7k, 5k) \mid k \in \mathbb{Z}\}.$$

Correction de l'exercice 15

Déterminer les solutions de l'équation (E') : $6u + 11v = 7$.

- **Recherche d'une solution particulière**
  Puisque $(2\ ;\ -1)$ est une solution particulière de l'équation

  $$(E)\ :\ 6u + 11v = 1$$

  Alors

  $$6\times\ 2 + 11\times(\ -1) = 1$$

  En multipliant les deux membres de l'égalité par 7 on obtient :

  $$6\times\ 2\times 7 + 11\times(\ -1)\times 7 = 7$$

  Et donc

  $$6\times\ 14 + 11\times(\ -7) = 7$$

  Ainsi $(14\ ;\ -7)$ est une solution particulière de l'équation $(E')\ :\ 6u + 11v = 7$.

- **Solutions générales**
  On utilise la même méthode :

  – **Transformation de l'équation**

  $$(E')\ :\ 6u + 11v = 7$$

  Puisque le couple $(14\ ;\ -7)$ est une solution particulie de l'équation (E') on a : $6\times\ 14 + 11\times(\ -7) = 7$.
  Donc

  $$\begin{cases} 6\times u & + & 11\times v & = 7 \\ 6\times\ 14 & + & 11\times(\ -7) & = 7 \end{cases} \underset{\text{par soustraction}}{\Longrightarrow} 6(u\ -14) + 11(v +\ \ 7) = 0$$

  Donc l'équation (E') devient :

  $$(E')\ :\ 6(u\ -14) = -11(v +\ \ 7)$$

  – **Application du théorrme de Gauss**

  Théorème 3 (Carl Friedrich Gauss, 1777-1855)

  Soit a, b, c des entiers.

  Si $\begin{cases} a \text{ divise le produit } bc \\ a \text{ et } b \text{ sont premiers entre eux} \end{cases}$, alors a divise c.

  

  Remarque : Le mathématicien allemand Carl Friedrich Gauss énonce et prouve ce théorrme (sous forme de lemme en fait) en 1801 dans son ouvrage « *Disquisitiones arithmeticae* ».

  $$(E')\ :\ 6(u\ -14) = -11(v +\ \ 7)$$

  Puisque 6 et 11 sont premiers entre eux, alors en appliquant le théorrme de Gauss :

  $$\begin{cases} 6 \text{ divise le produit } 11(v +\ \ 7) \\ 6 \text{ et } 11 \text{ sont premiers entre eux} \end{cases} \underset{\text{d'aprrs le th. de Gauss}}{\Longrightarrow} 6 \text{ divise } (v +\ \ 7)$$

  $$\begin{cases} 11 \text{ divise le produit } 6(u\ -14) \\ 6 \text{ et } 11 \text{ sont premiers entre eux} \end{cases} \underset{\text{d'aprrs le th. de Gauss}}{\Longrightarrow} 11 \text{ divise } (u\ -14)$$

  Il existe donc des entiers k et k' tels que :

  $$\begin{cases} (v +\ \ 7) & = 6k \\ (u\ -14) & = -11k' \end{cases}$$

  En reportant dans l'équation (E') on obtient

  $$6\times 11k' = 11\times 6k \Longleftrightarrow k = k'$$

  Ainsi, les solutions de l'équation (E') sont les couples de la forme

  $$\boxed{(14 - 11k\ \ ;\ -7 + 6k)\ ;\ k \in \mathbb{Z}}$$

Correction de l'exercice 16

Déterminer les solutions de l'équation (E') : $5u+7v=8$.

- **Recherche d'une solution particulière**
  Puisque $(3\ ;\ -2)$ est une solution particulière de l'équation

  $$(E)\ :\ 5u+7v=1$$

  Alors

  $$5\times\ 3+7\times(\ -2)=1$$

  En multipliant les deux membres de l'égalité par 8 on obtient :

  $$5\times\ 3\times 8+7\times(\ -2)\times 8=8$$

  Et donc

  $$5\times\ 24+7\times(\ -16)=8$$

  Ainsi $(24\ ;\ -16)$ est une solution particulière de l'équation $(E')\ :\ 5u+7v=8$.

- **Solutions générales**
  On utilise la même méthode :

  – **Transformation de l'équation**

  $$(E')\ :\ 5u+7v=8$$

  Puisque le couple $(24\ ;\ -16)$ est une solution particulie de l'équation (E') on a : $5\times\ 24+7\times(\ -16)=8$.
  Donc

  $$\begin{cases} 5\times u & + & 7\times v & = 8 \\ 5\times\ 24 & + & 7\times(\ -16) & = 8 \end{cases} \underset{\text{par soustraction}}{\Longrightarrow} 5(u\ -24)+7(v+\ \ 16)=0$$

  Donc l'équation (E') devient :

  $$(E')\ :\ 5(u\ -24)=-7(v+\ \ 16)$$

  – **Application du théorrme de Gauss**

  Théorème 4 (Carl Friedrich Gauss, 1777-1855)

  Soit a, b, c des entiers.

  Si $\begin{cases} a \text{ divise le produit } bc \\ a \text{ et } b \text{ sont premiers entre eux} \end{cases}$, alors a divise c.

  

  Remarque : Le mathématicien allemand Carl Friedrich Gauss énonce et prouve ce théorrme (sous forme de lemme en fait) en 1801 dans son ouvrage « *Disquisitiones arithmeticae* ».

  $$(E')\ :\ 5(u\ -24)=-7(v+\ \ 16)$$

  Puisque 5 et 7 sont premiers entre eux, alors en appliquant le théorrme de Gauss :

  $$\begin{cases} 5 \text{ divise le produit } 7(v+\ \ 16) \\ 5 \text{ et } 7 \text{ sont premiers entre eux} \end{cases} \underset{\text{d'aprrs le th. de Gauss}}{\Longrightarrow} 5 \text{ divise } (v+\ \ 16)$$

  $$\begin{cases} 7 \text{ divise le produit } 5(u\ -24) \\ 5 \text{ et } 7 \text{ sont premiers entre eux} \end{cases} \underset{\text{d'aprrs le th. de Gauss}}{\Longrightarrow} 7 \text{ divise } (u\ -24)$$

  Il existe donc des entiers k et k' tels que :

  $$\begin{cases} (v+\ \ 16) & = 5k \\ (u\ -24) & = -7k' \end{cases}$$

En reportant dans l'équation (E') on obtient

$$5 \times 7k' = 7 \times 5k \iff k = k'$$

Ainsi, les solutions de l'équation (E') sont les couples de la forme

$$\boxed{\big(24 - 7k \ \ ; \ -16 + 5k\big) \ ; \ k \in \mathbb{Z}}$$