3 PGCD & Théorème de Bézout

On désigne par $\mathrm{D}(a,b)$ l'ensemble des diviseurs communs à deux entiers a et b.

3.1 Déterminer :

1) $\mathrm{D}(12,18)$
2) $\mathrm{D}(45,75)$

3.2 Montrer que $\mathrm{D}(a,b)=\mathrm{D}(a-k\,b,b)$ pour tout $k\in\mathbb{Z}$.

Indication : il s'agit plus précisément de montrer deux inclusions :

1) $\mathrm{D}(a,b)\subset\mathrm{D}(a-k\,b,b)$
   Si $d\in\mathrm{D}(a,b)$, alors $d\in\mathrm{D}(a-k\,b,b)$.
   En d'autres termes, si d divise a et si d divise b, alors d divise $a-k\,b$ et d divise b.
2) $\mathrm{D}(a-k\,b,b)\subset\mathrm{D}(a,b)$
   Si $d\in\mathrm{D}(a-k\,b,b)$, alors $d\in\mathrm{D}(a,b)$.
   En d'autres termes, si d divise $a-k\,b$ et si d divise b, alors d divise a et d divise b.

3.3 Montrer que $\mathrm{D}(a,b)=\mathrm{D}(r,b)$ où r désigne le reste de la division euclidienne de a par b.

Si a et b sont deux entiers relatifs non tous deux nuls, alors $\mathrm{D}(a,b)$ est non vide ($1\in\mathrm{D}(a,b)$) et fini, car il ne contient que des entiers entre $-a$ et a ou entre $-b$ et b. Par conséquent $\mathrm{D}(a,b)$ possède un plus grand élément : on l'appelle le *plus grand commun diviseur* de a et b et on le note $\mathrm{pgcd}(a,b)$.

Remarque : $\mathrm{pgcd}(a,b)=\mathrm{pgcd}(b,a)=\mathrm{pgcd}\big(|a|,|b|\big)$
Lorsque l'on doit calculer $\mathrm{pgcd}(a,b)$, on peut donc supposer a et b positifs, ce que nous ferons dorénavant.

3.4 Calculer :

1) $\mathrm{pgcd}(308,448)$
2) $\mathrm{pgcd}(120,264)$

Algorithme d'Euclide

Étant donné deux entiers positifs a et b, effectuons la suite de divisions euclidiennes suivante :

$$\begin{array}{rcrll}
a &=& b\cdot q_1 & +\ r_1 & (r_1\neq 0)\\
b &=& r_1\cdot q_2 & +\ r_2 & (r_2\neq 0)\\
r_1 &=& r_2\cdot q_3 & +\ r_3 & (r_3\neq 0)\\
 & & \vdots & & \\
r_{n-2} &=& r_{n-1}\cdot q_n & +\ r_n & (r_n\neq 0)\\
r_{n-1} &=& r_n\cdot q_{n+1} & &
\end{array}$$

Alors $\mathrm{pgcd}(a,b)=r_n$.

3.5 1) À l'aide de l'exercice 3.3, montrer que $\text{pgcd}(a, b) = \text{pgcd}(b, r)$ où r est le reste de la division euclidienne de a par b.

2) Démontrer l'algorithme d'Euclide.

3.6 Appliquer l'algorithme d'Euclide à l'exercice 3.4.

3.7 À l'aide de l'algorithme d'Euclide, calculer :

1) $\text{pgcd}(528, 312)$

2) $\text{pgcd}(-286, 390)$

3) $\text{pgcd}(538, 392)$

4) $\text{pgcd}(22680, 3528, 11088)$

Deux nombres entiers a et b sont dits **premiers entre eux** si $\text{pgcd}(a, b) = 1$.

3.8 Montrer que n^2 et $n + 1$ sont premiers entre eux quel que soit $n \in \mathbb{Z}$.

Théorème de Bézout

Soient a et b deux entiers relatifs non tous les deux nuls et $d = \text{pgcd}(a, b)$. Alors il existe deux entiers x et y tels que $a\,x + b\,y = d$.

Preuve Appliquons l'algorithme d'Euclide et résolvons toutes ces équations (sauf la dernière) relativement aux restes successifs :

$$\begin{array}{rcrcl}
a = & b \cdot q_1 & + r_1 & \Longrightarrow & r_1 = a - b \cdot q_1 \\
b = & r_1 \cdot q_2 & + r_2 & \Longrightarrow & r_2 = b - r_1 \cdot q_2 \\
r_1 = & r_2 \cdot q_3 & + r_3 & \Longrightarrow & r_3 = r_1 - r_2 \cdot q_3 \\
 & \vdots & & & \vdots \\
r_{n-3} = & r_{n-2} \cdot q_{n-1} & + r_{n-1} & \Longrightarrow & r_{n-1} = r_{n-3} - r_{n-2} \cdot q_{n-1} \\
r_{n-2} = & r_{n-1} \cdot q_n & + d & \Longrightarrow & d = r_{n-2} - r_{n-1} \cdot q_n \\
r_{n-1} = & d \cdot q_{n+1} & & &
\end{array}$$

En partant de la dernière égalité, et en remontant, remplaçons successivement chaque r_i $(n - 1 \geqslant i \geqslant 1)$ par sa valeur tirée de l'équation précédente :

$$\begin{aligned}
d &= r_{n-2} - r_{n-1} \cdot q_n \\
&= r_{n-2} - (r_{n-3} - r_{n-2} \cdot q_{n-1}) \cdot q_n = r_{n-3} \underbrace{(-q_n)}_{x_n} + r_{n-2} \underbrace{(1 + q_{n-1}\, q_n)}_{y_n} \\
&= r_{n-3}\, x_n + r_{n-2}\, y_n \\
&= r_{n-3}\, x_n + (r_{n-4} - r_{n-3}\, q_{n-2})\, y_n = r_{n-4} \underbrace{y_n}_{x_{n-1}} + r_{n-3} \underbrace{(x_n - q_{n-2}\, y_n)}_{y_{n-1}} \\
&= r_{n-4}\, x_{n-1} + r_{n-3}\, y_{n-1} \\
&\vdots \\
&= r_1\, x_3 + r_2\, y_3
\end{aligned}$$

$$
\begin{aligned}
&= r_1\,x_3 + (b - r_1\,q_2)\,y_3 = b\,\underbrace{y_3}_{x_2} + r_1\,\underbrace{(x_3 - q_2\,y_3)}_{y_2} \\
&= b\,x_2 + r_1\,y_2 \\
&= b\,x_2 + (a - b\,q_1)\,y_2 = a\,\underbrace{y_2}_{x} + b\,\underbrace{(x_2 - q_1\,y_2)}_{y} \\
&= a\,x + b\,y
\end{aligned}
$$

3.9 À partir des calculs de l'exercice 3.6, déterminer des entiers x et y tels que :

1) $308\,x + 448\,y = 28$ 2) $120\,x + 264\,y = 24$

Théorème de Bachet de Mériziac

Soient a et b deux entiers relatifs non tous les deux nuls et $d = \text{pgcd}(a, b)$. L'ensemble des combinaisons linéaires entières de a et b coïncide avec l'ensemble des multiples de d :

$$\{a\,x + b\,y : x, y \in \mathbb{Z}\} = \{k\,d : k \in \mathbb{Z}\}$$

3.10 Démontrer le théorème de Bachet de Mériziac :

1) Soient $x, y \in \mathbb{Z}$. Montrer que d divise $a\,x + b\,y$.
2) Soit $k \in \mathbb{Z}$. Montrer, à l'aide du théorème de Bézout, qu'il existe des entiers x et y tels que $a\,x + b\,y = k\,d$.

3.11

1) Soit $n \in \mathbb{Z}$.
   (a) Simplifier $2\,(5\,n + 3) - 5\,(2\,n + 1)$.
   (b) Que peut-on en déduire pour les entiers $5\,n + 3$ et $2\,n + 1$?
2) Démontrer que les entiers a et b sont premiers entre eux :
   (a) $a = -n + 4$ $b = 3\,n - 11$
   (b) $a = 6\,n + 3$ $b = 3\,n + 1$
   (c) $a = 2\,n - 1$ $b = -7\,n + 3$

3.12 Soient a et b deux entiers et $d = \text{pgcd}(a, b)$. Montrer que $\dfrac{a}{d}$ et $\dfrac{b}{d}$ sont premiers entre eux.

3.13 Soient p et q deux entiers non nuls. Démontrer qu'il existe deux entiers a et b tels que $\dfrac{1}{p\,q} = \dfrac{a}{p} + \dfrac{b}{q}$ si et seulement si p et q sont premiers entre eux.

Lemme de Gauss

Soient a, b, c des entiers non nuls. Si a divise $b\,c$ et si a est premier avec b, alors a divise c.

3.14 Démontrer le lemme de Gauss grâce au théorème de Bézout.

Équations diophantiennes

Une *équation diophantienne* linéaire à deux variables est une équation de la forme $a\,x + b\,y = c$ où $a, b, c \in \mathbb{Z}$ et dont les solutions doivent être entières.

Théorème de résolution des équations diophantiennes

Soient $a, b \in \mathbb{Z}$, $d = \mathrm{pgcd}(a, b)$ et l'équation diophantienne $a\,x + b\,y = c$. Alors

1) *si d ne divise pas c, l'équation diophantienne $a\,x + b\,y = c$ n'a pas de solution.*
2) *si d divise c, l'équation diophantienne $a\,x + b\,y = c$ a une infinité de solutions ; de plus, si $(x_0\,;y_0)$ est une solution particulière, alors toutes les solutions sont données par $x = x_0 + \frac{b}{d}\,k$ et $y = y_0 - \frac{a}{d}\,k$ $(k \in \mathbb{Z})$.*

3.15 Le but de cet exercice est de prouver le théorème de résolution des équations diophantiennes.

1) Prouver la contraposée de la première affirmation : si l'équation diophantienne $a\,x + b\,y = c$ admet une solution, alors d divise c.
2) Supposons que d divise c.
   (a) Montrer que le théorème de Bézout garantit l'existence d'une solution particulière : il existe des entiers x_0 et y_0 tels que $a\,x_0 + b\,y_0 = c$.
   (b) Vérifier que l'équation diophantienne $a\,x + b\,y = c$ admet pour solution $x = x_0 + \frac{b}{d}\,k$ et $y = y_0 - \frac{a}{d}\,k$ pour tout $k \in \mathbb{Z}$.
   (c) Il reste encore à montrer que toutes les solutions de l'équation diophantienne sont de cette forme. Soient $x, y \in \mathbb{Z}$ avec $a\,x + b\,y = c$.
      i. Puisque $a\,x_0 + b\,y_0 = c$, vérifier que la soustraction de ces équations donne $a\,(x - x_0) = b\,(-y + y_0)$, puis $\frac{a}{d}\,(x - x_0) = \frac{b}{d}\,(-y + y_0)$.
      ii. En déduire, grâce à l'exercice 3.12 et au lemme de Gauss, que $\frac{a}{d}$ divise $-y + y_0$.
      iii. En conclure qu'il existe $k \in \mathbb{Z}$ tel que $y = y_0 - \frac{a}{d}\,k$.
      iv. Après substitution dans l'équation $\frac{a}{d}\,(x - x_0) = \frac{b}{d}\,(-y + y_0)$, constater que $x = x_0 + \frac{b}{d}\,k$.

3.16 Déterminer toutes les solutions entières des équations suivantes :

1) $42\,x + 25\,y = 3$
2) $153\,x - 102\,y = 413$
3) $45\,x + 27\,y = 117$
4) $120\,x + 43\,y = 12$

3.17 Peut-on trouver sur la droite d'équation $35\,x + 84\,y = 150$ des points à coordonnées entières ?

3.18 Les pièces de 1 franc ont un diamètre de 23 mm, celles de 50 centimes un diamètre de 18 mm. En alignant de telles pièces, peut-on obtenir une longueur égale à :

1) 1 dm 2) 1 m

Si oui, quelle est, dans chaque cas, la solution la plus économique ?

3.19 Un homme veut obtenir des chèques pour un montant de 500 €. Les seuls montants disponibles pour ces chèques sont 20 € et 50 €. Comment doit-il s'y prendre ? Donner toutes les solutions.

3.20 On doit à Euler le petit problème suivant :

> Un soir dans une auberge s'arrêtent plusieurs diligences. Des hommes et des femmes, moins nombreuses, s'attablent. Chaque homme doit payer 19 sous et chaque femme 13 sous. Sachant qu'à la fin du repas, l'aubergiste a récolté exactement 1000 sous, retrouvez combien d'hommes et de femmes ont mangé à l'auberge ce jour-là.

Réponses

3.1 1) $\mathrm{D}(12, 18) = \{\pm 1\,;\pm 2\,;\pm 3\,;\pm 6\}$ 2) $\mathrm{D}(45, 75) = \{\pm 1\,;\pm 3\,;\pm 5\,;\pm 15\}$

3.4 1) 28 2) 24

3.7 1) 24 2) 26 3) 2 4) 504

3.9 1) $308 \cdot 3 + 448 \cdot (-2) = 28$ 2) $120 \cdot (-2) + 264 \cdot 1 = 24$

3.11 1) (a) $2\,(5\,n + 3) - 5\,(2\,n + 1) = 1$

(b) $5\,n + 3$ et $2\,n + 1$ sont premiers entre eux

2) (a) $3\,a + b = 1$ (b) $a - 2\,b = 1$ (c) $-7\,a - 2\,b = 1$

3.16 1) $\mathrm{S} = \big\{(9 - 25\,k\,; -15 + 42\,k) : k \in \mathbb{Z}\big\}$

2) $\mathrm{S} = \varnothing$

3) $\mathrm{S} = \big\{(2 + 3\,k\,; 1 - 5\,k) : k \in \mathbb{Z}\big\}$

4) $\mathrm{S} = \big\{(228 + 43\,k\,; -636 - 120\,k) : k \in \mathbb{Z}\big\}$

3.17 Non

3.18 1) 2 fois 1 fr. et 3 fois 50 ct. 2) 2 fois 1 fr. et 53 fois 50 ct.

3.19 $5\,k$ chèques de 20 € et $10 - 2\,k$ chèques de 50 € avec $0 \leqslant k \leqslant 5$

3.20 41 hommes et 17 femmes