Chapitre 4

Les équations diophantiennes

Les nombres réels sont très utiles, mais parfois on préfère résoudre des problèmes qui nécessitent des solutions à valeurs entières. Voici deux problèmes nécessitant l'utilisation d'outils spécifiquement élaborés pour résoudre des problèmes sur les entiers.

1. Un cinéma vend deux sortes de tickets : ceux à 12 CHF et ceux à 17 CHF.

   Un soir, la caissière constate qu'elle a encaissé 285 CHF, mais elle ne se souvient pas du nombre de billets de chaque sorte qu'elle a vendus.

   Est-il possible de le lui dire ? Et si le ticket le plus cher valait 18 CHF ?

2. On dispose de deux sabliers : un à 4 minutes, l'autre à 7 minutes. Comment faire pour déterminer un temps de 9 minutes ?

4.1 Calcul du pgcd, algorithme d'Euclide

Définition

Soit a et b deux nombres entiers.

On définit le *plus grand commun diviseur de a et b*, noté $\text{pgcd}(a, b)$, comme étant le plus grand nombre positif qui divise à la fois a et b.

Exemples

1. On a $\text{pgcd}(12, 14) = 2$.

   En effet, l'ensemble des diviseurs de 12 est $D_{12} = \{1, 2, 3, 4, 6, 12\}$ et l'ensemble des diviseurs de 14 est $D_{14} = \{1, 2, 7, 14\}$. L'ensemble des diviseurs commun à 12 et à 14 est donc $D_{12} \cap D_{14} = \{1, 2\}$. Ainsi, le plus grand commun diviseur est 2.

2. On a aussi $\text{pgcd}(2, 3) = 1$.

3. Ou encore $\text{pgcd}(7, -21) = 7$.

4. On a $\text{pgcd}(0, b) = b$ si $b \neq 0$, car 0 est divisible par tout nombre. On utilise la convention $\text{pgcd}(0, 0) = 0$ pour respecter la règle précédente (voir aussi le théorème de Bezout en page 25).

Définition. Deux nombres a et b tels que $\text{pgcd}(a, b) = 1$ sont dit *premiers entre-eux.*

Résultat

Soit a et b deux nombres entiers avec $b \neq 0$. En effectuant la division euclidienne de a par b, on obtient un quotient q et un reste r tels que $a = qb + r$ (et $0 \leqslant r < |b|$). Alors

$$\boxed{\text{pgcd}(a, b) = \text{pgcd}(b, r)}$$

Preuve

1. $\text{pgcd}(b, r) \leqslant \text{pgcd}(a, b)$.

   Pour montrer cela, il suffit de montrer que $\text{pgcd}(b, r)$ divise a et b. Ainsi, il sera bien plus petit ou égal au plus grand commun diviseur de a et de b, noté $\text{pgcd}(a, b)$.

   Or, il est évident que $\text{pgcd}(b, r)$ divise b et r (par définition). Ainsi il divise aussi qb et r, donc $\text{pgcd}(b, r)$ divise $a = qb + r$.

2. $\text{pgcd}(a, b) \leqslant \text{pgcd}(b, r)$.

   Pour montrer cela, il suffit de montrer que $\text{pgcd}(a, b)$ divise b et r. Ainsi, il sera bien plus petit ou égal au plus grand commun diviseur de b et de r, noté $\text{pgcd}(b, r)$.

   Or, il est évident que $\text{pgcd}(a, b)$ divise a et b (par définition). Ainsi il divise aussi a et qb, donc $\text{pgcd}(a, b)$ divise $r = a - qb$.

On a ainsi montré que $\text{pgcd}(b, r) \leqslant \text{pgcd}(a, b) \leqslant \text{pgcd}(b, r)$. Il est donc évident que $\text{pgcd}(a, b) = \text{pgcd}(b, r)$. □

4.1.1 L'algorithme d'Euclide

Soit a et b deux nombres entiers non nuls. Grâce au résultat précédent, on peut en effectuant des divisions euclidiennes successives calculer $\text{pgcd}(a, b)$.

$$\begin{array}{llll}
\text{comme } b \neq 0, & a = bq_1 + r_1, & \text{pgcd}(a, b) = \text{pgcd}(b, r_1), & 0 \leqslant r_1 < |b| \\
\text{si } r_1 \neq 0, & b = r_1 q_2 + r_2, & \text{pgcd}(b, r_1) = \text{pgcd}(r_1, r_2), & 0 \leqslant r_2 < r_1 \\
\text{si } r_2 \neq 0, & r_1 = r_2 q_3 + r_3, & \text{pgcd}(r_1, r_2) = \text{pgcd}(r_2, r_3), & 0 \leqslant r_3 < r_2 \\
 & & \cdots & \\
\text{si } r_{n-1} \neq 0, & r_{n-2} = r_{n-1} q_n + r_n, & \text{pgcd}(r_{n-2}, r_{n-1}) = \text{pgcd}(r_{n-1}, r_n), & 0 = r_n < r_{n-1} \\
\text{si } r_n = 0, & & \text{pgcd}(r_{n-1}, r_n) = \text{pgcd}(r_{n-1}, 0) = r_{n-1} &
\end{array}$$

On a ainsi construit une suite d'égalité

$$\text{pgcd}(a, b) = \text{pgcd}(b, r_1) = \text{pgcd}(r_1, r_2) = \cdots = \text{pgcd}(r_{n-2}, r_{n-1}) = \text{pgcd}(r_{n-1}, r_n) = r_{n-1}$$

où le premier reste nul est r_n. Dans ce cas $\text{pgcd}(a, b)$ est égal au dernier reste non nul. Comme les restes forment une suite de nombres naturels strictement décroissante, il est certain qu'il y aura un premier reste nul (noté ici r_n).

Voici l'algorithme d'Euclide en JavaScript et en Python respectivement.

```
function euclide(a,b)
   {while ( b != 0 )
       {reste = a % b
        a = b
        b = reste
       }
   return a
   }
```

```
def euclide(a,b) :
    while ( b != 0 ) :
        reste = a % b
        a = b
        b = reste

    return a
```

4.2 Théorème de Bezout, algorithme d'Euclide étendu

4.2.1 Théorème de Bezout

Soit a et b deux nombres entiers.

Alors, il existe deux nombres entiers x et y tels que $ax + by = \text{pgcd}(a, b)$.

Preuve

L'algorithme d'Euclide étendu décrit ci-dessous permet de trouver les entiers x et y. □

4.2.2 L'algorithme d'Euclide étendu

Cet algorithme consiste à compléter l'algorithme d'Euclide.

Algorithme (la preuve est en annexe en page 32)

Il s'agit d'un tableau à quatre colonnes : la première colonne correspond à l'algorithme d'Euclide ; la dernière colonne est celle des quotients. Dans les deux colonnes au milieu, on place (de gauche à droite et de haut en bas) les nombres 1, 0, 0, 1. On peut choisir de remplir le tableau colonne par colonne en commençant par la première et la dernière colonne, on peut aussi remplir le tableau ligne par ligne. Les trois premières colonnes se construisent de manière similaire : on calcule le nombre suivant (en gris clair) à l'aide des deux nombres qui se trouvent juste en dessus et le quotient (en gris), comme montré ci-dessous. L'algorithme est terminé lorsqu'on a rempli la ligne du reste nul, notée (♢).

		a	b	
	a	1	0	quotients
	b	0	1	q_1
	$r_1 = a - bq_1$	$1 - 0q_1$	$0 - 1q_1$	q_2
	...	...	...	...
	r_{i-1}	s_i	t_i	q_i
	r_i	u_i	v_i	q_{i+1}
	$r_{i+1} = r_{i-1} - r_i q_{i+1}$	$s_i - u_i q_{i+1}$	$t_i - v_i q_{i+1}$	q_{i+2}
	...	...	...	...
(♡)	$r_{n-1} = \text{pgcd}(a, b)$	s_n	t_n	q_n
(♢)	$r_n = 0$	u_n	v_n	

On trouve à la ligne (♡) la combinaison de Bezout et un bonus à la ligne (♢).

$$(♡) : a \cdot s_n + b \cdot t_n = \text{pgcd}(a, b) \quad \text{et} \quad (♢) : a \cdot u_n + b \cdot t_n = 0$$

Exemple

On cherche la combinaison de Bezout pour $a = 28$ et $b = 6$.

		28	6	
	28	1	0	quotients
	6	0	1	4
	4	1	−4	1
(♡)	pgcd(28, 6) = 2	−1	5	2
(♢)	0	3	−14	

Ainsi, on a :

$$\begin{cases} \text{Bezout} & (\heartsuit): & 28 \cdot (-1) & + & 6 \cdot & 5 & = & 2 \\ & (\diamondsuit): & 28 \cdot & 3 & + & 6 \cdot (-14) & = & 0 \end{cases}$$

Remarque

À chaque ligne, on retrouve le terme de gauche en écrivant la combinaison avec les deux termes du milieu.

	a	b	
a	1	0	quotients
b	0	1	
...	...	...	
r	s	t	
...	...	...	

Autrement dit, quelque soit la ligne, on a :

$$r = a \cdot s + b \cdot t$$

Cette propriété, démontrée en page 34, permet de repérer les éventuelles erreurs de calcul.

4.2.3 Lemme de Gauss (généralisation du lemme d'Euclide)

Soit a et b deux nombres entiers.

Si c est un nombre tel que $\text{pgcd}(c, a) = 1$ et tel que c divise ab, alors c divise b.

Preuve

Par le théorème de Bezout, il existe deux nombres entiers x et y tels que

$$c \cdot x + a \cdot y = 1$$

En multipliant cette équation par b, on obtient :

$$\underbrace{c \cdot x \cdot b}_{\text{divisible par } c} + \underbrace{a \cdot y \cdot b}_{\text{divisible par } c, \text{ car } c \text{ divise } ab} = b$$

Donc b est divisible par c. □

4.3 Les équations diophantiennes

Définition

Soit a, b et c trois nombres entiers. L'équation $ax+by=c$ est une *équation diophantienne* si les solutions cherchées x et y sont des nombres entiers.

Résultat d'existence d'une solution

Soit a et b deux nombres entiers. On a l'équivalence :

$$ax + by = c \text{ admet (au moins) une solution entière} \iff \text{pgcd}(a,b) \text{ divise } c$$

Preuve constructive

"$\Rightarrow$" Il est évident que $\text{pgcd}(a,b)$ divise ax et by, donc $\text{pgcd}(a,b)$ divise leur somme qui vaut c (car x et y sont solutions entières de l'équation $ax+by=c$).

"$\Leftarrow$" Par le théorème de Bezout, il existe deux nombres entiers m et n tels que :

$$am + bn = \text{pgcd}(a,b)$$

Ces deux nombres entiers m et n se trouvent grâce à l'algorithme d'Euclide étendu !

Par hypothèse, il existe $k \in \mathbb{Z}$ tel que $\text{pgcd}(a,b)k = c$ ($\Leftrightarrow k = \frac{c}{\text{pgcd}(a,b)}$). Ainsi en multipliant l'équation ci-dessus par k, on obtient :

$$a(mk) + b(nk) = \text{pgcd}(a,b)k = c$$

De ce fait, le couple $(x;y) = (mk;nk)$ est une solution de $ax+by=c$. □

Remarque importante

Avant de résoudre une équation diophantienne, on vérifie toujours si elle admet une solution en utilisant ce résultat d'existence. En effet, si l'équation n'admet pas de solution, alors le problème est clos. Alors que si elle possède une solution, il va falloir travailler pour toutes les trouver !

Recherche d'une solution particulière d'une équation diophantienne

Dans le cas où l'existence d'une solution est vérifiée, on peut commencer à chercher les solutions de l'équation diophantienne.

La méthode de recherche d'une solution particulière se trouve dans la preuve constructive du résultat d'existence d'une solution à l'équation diophantienne.

1. Grâce à l'algorithme d'Euclide étendu, on trouve une solution particulière $(m;n)$ de l'équation $ax+by=\text{pgcd}(a,b)$.
2. Pour trouver une solution particulière $(x_0;y_0)$ de l'équation $ax+by=c$, on multiplie m et n par $\frac{c}{\text{pgcd}(a,b)}$. Ainsi

$$(x_0;y_0) = \left(m \cdot \tfrac{c}{\text{pgcd}(a,b)}; n \cdot \tfrac{c}{\text{pgcd}(a,b)}\right)$$

Théorème de résolution d'une équation diophantienne

Soit l'équation diophantienne (ED) : $ax + by = c$ et $(x_0; y_0)$ une solution particulière. Soit aussi l'*équation homogène associée* (EH) : $ax + by = 0$. On a

1. Si $(x_h; y_h)$ est une solution de (EH), alors $(x_h + x_0; y_h + y_0)$ est une solution de (ED).
2. Si $(x; y)$ est une solution de (ED), alors $(x - x_0; y - y_0)$ est une solution de (EH).

Autrement dit, à travers la solution particulière $(x_0; y_0)$, à chaque solution de (ED) correspond une unique solution de (EH) et réciproquement.

Preuve

On suppose qu'on connaît une solution particulière $(x_0; y_0)$ de l'équation (ED).
On doit montrer :

1. Si $(x_h; y_h)$ est une solution de (EH), alors $(x; y) = (x_h + x_0; y_h + y_0)$ est une solution de (ED).

   Il suffit de vérifier (ED) pour $(x; y)$.

   $$ax + by = a(x_h + x_0) + b(y_h + y_0) = \underbrace{ax_h + by_h}_{= 0 \text{ car } (x_h; y_h) \text{ est solution de } (EH)} + \overbrace{ax_0 + by_0}^{= c \text{ car } (x_0; y_0) \text{ est solution de } (ED)} = c$$

   Ainsi, $(x; y)$ est bien une solution de l'équation diophantienne (ED).

2. Si $(x; y)$ est une solution de (ED), alors $(x_h; y_h) = (x - x_0; y - y_0)$ est une solution de (EH).

   Il suffit de vérifier (EH) pour $(x_h; y_h)$.

   $$ax_h + by_h = a(x - x_0) + b(y - y_0) = \underbrace{ax + by}_{= c \text{ car } (x; y) \text{ est solution de } (ED)} - \overbrace{\left(ax_0 + by_0\right)}^{= c \text{ car } (x_0; y_0) \text{ est solution de } (ED)} = 0$$

   Ainsi, $(x_h; y_h)$ est bien une solution de l'équation homogène (EH). □

Solution générale de l'équation diophantienne

Lorsque $\text{pgcd}(a, b)$ divise c, les solutions de l'équation diophantienne $ax + by = c$ sont

$$\begin{cases} x = \boxed{x_0} \boxed{- \dfrac{b}{\text{pgcd}(a,b)} k} \\ y = \boxed{y_0} \boxed{+ \dfrac{a}{\text{pgcd}(a,b)} k} \end{cases}, \quad k \in \mathbb{Z}$$

Solution particulière (voir page précédente) ↑ — ↑ Solution générale de l'équation homogène (voir preuve page suivante)

Slogans

1. À chaque solution correspond un unique k (le même pour les deux équations).
2. À chaque nombre entier k correspond une unique solution.

Preuve

Le théorème de résolution permet d'énoncer la solution générale de l'équation diophantienne dès qu'on connaît une solution particulière et la solution générale de l'équation homogène. Ci-dessous, on démontre que la solution générale de l'équation homogène $ax + by = 0$ est bien celle précitée.

1. D'abord, on montre que les solutions entières de $ax + by = 0$ s'écrivent comme

$$x = -\frac{b}{\text{pgcd}(a,b)}k \quad \text{et} \quad y = \frac{a}{\text{pgcd}(a,b)}k \quad \text{avec} \quad k \in \mathbb{Z}$$

   Pour cela, on distingue :

   (a) Si $a \neq 0$ et $\text{pgcd}(a,b) = 1$.

   Dans ce cas, on a $-ax = by$, ainsi a divise by, mais comme $\text{pgcd}(a,b) = 1$, par le lemme de Gauss, on sait que a divise y (ou que y est un multiple de a).

   Par conséquent, $y = ak$ avec $k \in \mathbb{Z}$ et ainsi :

$$\begin{cases} ax + by = 0 \\ y = ak \end{cases} \overset{\text{subst.}}{\iff} \begin{cases} ax + bak = 0 \\ y = ak \end{cases} \iff \begin{cases} a(x + bk) = 0 \\ y = ak \end{cases}$$

$$\overset{a\neq 0}{\iff} \begin{cases} x + bk = 0 \\ y = ak \end{cases} \iff \begin{cases} x = -bk \\ y = ak \end{cases}$$

   On a donc les solutions désirées, puisque dans ce cas, on a $\text{pgcd}(a,b) = 1$.

   (b) Si $a \neq 0$ et $\text{pgcd}(a,b) \neq 1$.

   On se ramène au cas précédent en divisant l'équation $ax+by = 0$ par $\text{pgcd}(a,b)$.

$$ax + by = 0 \overset{:\text{pgcd}(a,b)}{\iff} \frac{a}{\text{pgcd}(a,b)}x + \frac{b}{\text{pgcd}(a,b)}y = 0$$

   On se trouve bien dans le cas précédent car $\text{pgcd}\left(\frac{a}{\text{pgcd}(a,b)}, \frac{b}{\text{pgcd}(a,b)}\right) = 1$. Donc, il existe $k \in \mathbb{Z}$, tel que

$$x = -\frac{b}{\text{pgcd}(a,b)}k \quad \text{et} \quad y = \frac{a}{\text{pgcd}(a,b)}k \quad \text{avec} \quad k \in \mathbb{Z}$$

   (c) Dans le cas où $a = 0$, c'est b qui est non nul, et on effectue les raisonnements symétriques (en échangeant les rôles de a et b).

2. Il faut encore montrer que les valeurs

$$x = -\frac{b}{\text{pgcd}(a,b)}k \quad \text{et} \quad y = \frac{a}{\text{pgcd}(a,b)}k \quad \text{avec} \quad k \in \mathbb{Z}$$

   sont solutions de $ax + by = 0$ et ceci quelque soit la valeur de $k \in \mathbb{Z}$.

   C'est bien le cas, car

$$a \cdot \left(-\frac{b}{\text{pgcd}(a,b)}k\right) + b \cdot \left(\frac{a}{\text{pgcd}(a,b)}k\right) = -\frac{abk}{\text{pgcd}(a,b)} + \frac{abk}{\text{pgcd}(a,b)} = 0$$

□

Remarques

1. Puisque $\operatorname{pgcd}\left(\frac{a}{\operatorname{pgcd}(a,b)}, \frac{b}{\operatorname{pgcd}(a,b)}\right) = 1$, le pgcd des solutions de l'équation homogène est la valeur absolue de k.

   Par conséquent, si on a des solutions dont le pgcd vaut 1, alors ces solutions sont $x = -\frac{b}{\operatorname{pgcd}(a,b)}$ et $y = \frac{a}{\operatorname{pgcd}(a,b)}$, ou $x = \frac{b}{\operatorname{pgcd}(a,b)}$ et $y = -\frac{a}{\operatorname{pgcd}(a,b)}$ $(k = \pm 1)$.

2. Les deux dernières lignes de l'algorithme d'Euclide étendu sont très importantes.

		a	b	
	a	1	0	quotients
	b	0	1	q_1
	...	...	...	...
($\heartsuit$)	$\operatorname{pgcd}(a,b)$	m	n	q_n
($\diamondsuit$)	0	$\pm\frac{b}{\operatorname{pgcd}(a,b)}$	$\mp\frac{a}{\operatorname{pgcd}(a,b)}$	

   À la ligne ($\heartsuit$), on trouve une solution $(m; n)$ de l'équation $ax + by = \operatorname{pgcd}(a, b)$. Ainsi $(x_0; y_0) = (m \cdot \frac{c}{\operatorname{pgcd}(a,b)}; n \cdot \frac{c}{\operatorname{pgcd}(a,b)})$ est une solution particulière de l'équation diophantienne $ax + by = c$.

   À la ligne ($\diamondsuit$), on trouve (au signe près) les coefficients de k de la solution générale de l'équation homogène $ax + by = 0$. Pour démontrer que c'est bien le cas, il suffit de combiner la remarque précédente avec la conséquence du bas de la page 35.

Exemple

On désire résoudre l'équation diophantienne $34x + 16y = 14$.

1. On commence par vérifier si l'équation admet au moins une solution.

   C'est bien le cas car $\operatorname{pgcd}(34, 16) = 2$ divise 14.

2. Pour trouver la solution générale, on va calculer les lignes ($\heartsuit$) et ($\diamondsuit$) de l'algorithme d'Euclide étendu.

		34	16	
	34	1	0	quotients
	16	0	1	2
($\heartsuit$)	2	1	−2	8
($\diamondsuit$)	0	−8	17	

   Ainsi $(1; -2)$ est une solution particulière de l'équation $34x + 16y = \operatorname{pgcd}(34, 16)$, puisque la ligne ($\heartsuit$) dit que $34 \cdot 1 + 16 \cdot (-2) = 2$.

   Donc $(7; -14)$ est une solution particulière de $34x + 16y = 14$. En effet, on la trouve en multipliant par $7 = \frac{14}{\operatorname{pgcd}(34,16)}$ la solution de l'équation $34x + 16y = \operatorname{pgcd}(34, 16)$.

   En utilisant la ligne ($\diamondsuit$), on peut directement donner la solution générale de l'équation diophantienne $34x + 16y = 14$, qui est

$$\begin{cases} x = 7 - 8k \\ y = -14 + 17k \end{cases}, \quad k \in \mathbb{Z}$$

4.4 Annexe sur la relation entre les droites du plan et les équations diophantiennes

1. Dans le plan $\mathbb{R}^2$

Soit a, b, $c \in \mathbb{Z}$. L'équation $ax + by = c$ est l'équation d'une droite d dans le plan $\mathbb{R}^2$. Une solution particulière $P_0(x_0; y_0)$ est un point P_0 de cette droite. Dans le chapitre de géométrie du cours DF, il est démontré que le vecteur $\binom{-b}{a}$ est un vecteur directeur de cette droite. On donne ainsi une représentation paramétrique de la droite

$$d : \begin{cases} x = x_0 - bk \\ y = y_0 + ak \end{cases}, \quad k \in \mathbb{R}$$

2. Dans le réseau $\mathbb{Z}^2$

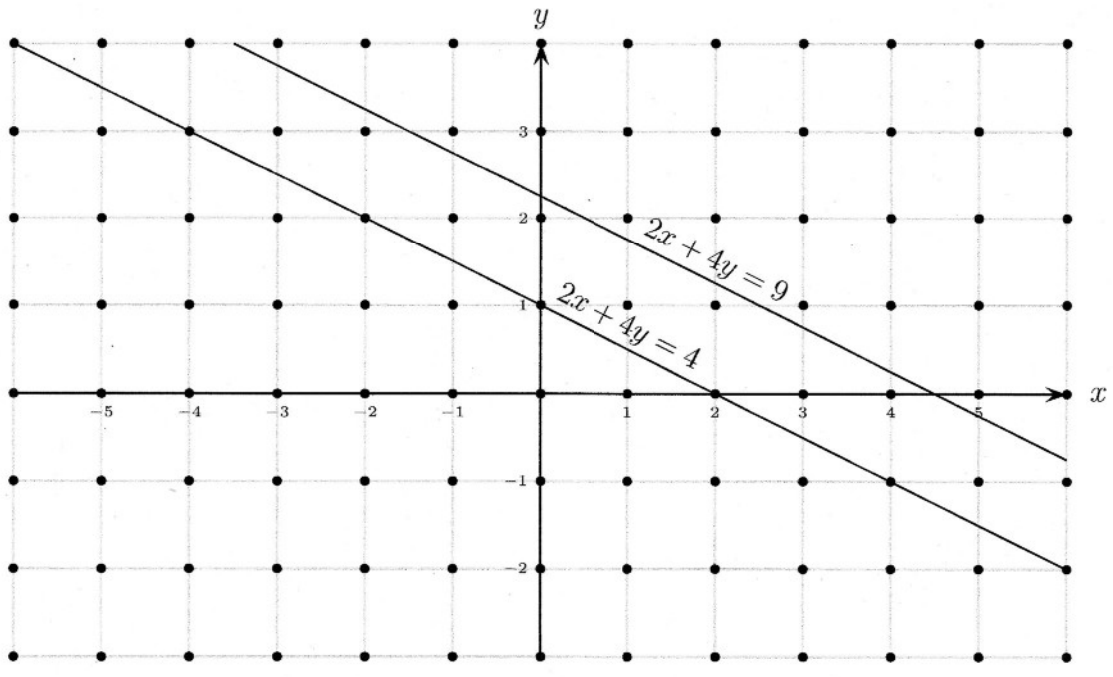
Soit a, b, $c \in \mathbb{Z}$. Le réseau $\mathbb{Z}^2$ est l'ensemble des points à coordonnées entières dans le plan $\mathbb{R}^2$. Lorsque $\text{pgcd}(a, b)$ divise c, on vient de voir que l'ensemble de solutions de l'équation diophantienne $ax + by = c$ est décrit par

$$\begin{cases} x = x_0 - \frac{b}{\text{pgcd}(a,b)}k \\ y = y_0 + \frac{a}{\text{pgcd}(a,b)}k \end{cases}, \quad k \in \mathbb{Z}$$

En fait, les vecteurs $\binom{-b}{a}$ et $\begin{pmatrix} -\frac{b}{\text{pgcd}(a,b)} \\ \frac{a}{\text{pgcd}(a,b)} \end{pmatrix}$ sont parallèles, mais le deuxième est, au signe près, le vecteur parallèle à $\binom{-b}{a}$ à composantes entières le plus court.

Exemple

Ci-dessous, on voit la droite $d_1 : 2x + 4y = 9$, qui ne passe par aucun point du réseau $\mathbb{Z}^2$, puisque $\text{pgcd}(2, 4) = 2$ ne divise pas 9. On voit aussi la droite $d_2 : 2x + 4y = 4$, qui passe par une infinité de point du réseau $\mathbb{Z}^2$ car $\text{pgcd}(2, 4) = 2$ divise 4. Son vecteur directeur à composantes entières le plus court est, au signe près, $\binom{-2}{1}$.



4.5 Annexe sur l'algorithme d'Euclide étendu

Cet algorithme consiste à reproduire l'algorithme d'Euclide en n'oubliant pas les quotients de chaque étape.

Pour établir cet algorithme, la notation et la multiplication des matrices de taille 2 fois 2 sont essentielles.

Etape 1 : $\text{pgcd}(a,b) = \text{pgcd}(b,r_1)$. On effectue la division euclidienne $a = bq_1 + r_1$ avec $0 \leqslant r_1 < |b|$. Ainsi, on a $r_1 = a - bq_1$ et à l'aide de la notation matricielle, on peut écrire l'expression suivante.

$$\begin{pmatrix} b \\ r_1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}$$

Etape 2 : $\text{pgcd}(b,r_1) = \text{pgcd}(r_1,r_2)$. On effectue la division euclidienne $b = r_1q_2 + r_2$ avec $0 \leqslant r_2 < r_1$. Ainsi, on a $r_2 = b - r_1q_2$ et à l'aide de la notation matricielle, on peut écrire l'expression suivante.

$$\begin{pmatrix} r_1 \\ r_2 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_2 \end{pmatrix} \begin{pmatrix} b \\ r_1 \end{pmatrix}$$

Etape n : $\text{pgcd}(r_{n-2},r_{n-1}) = \text{pgcd}(r_{n-1},r_n)$. On effectue la division euclidienne $r_{n-2} = r_{n-1}q_n + r_n$ avec $0 = r_n < r_{n-1}$. Ainsi, on a $r_n = r_{n-2} - r_{n-1}q_n$ et à l'aide de la notation matricielle, on peut écrire l'expression suivante.

$$\begin{pmatrix} \text{pgcd}(a,b) \\ 0 \end{pmatrix} = \begin{pmatrix} r_{n-1} \\ r_n \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_n \end{pmatrix} \begin{pmatrix} r_{n-2} \\ r_{n-1} \end{pmatrix}$$

On retrouve la multiplication matricielle [1]

Grâce aux étapes 1 et 2, on peut exprimer r_2 à l'aide de a et b (rappelons que le but de l'algorithme est d'exprimer r_{n-1} (qui est égal au pgcd) en fonction de a et b (voir l'énoncé du théorème de Bezout)).
En effet, on a $r_1 = a - bq_1$ et $r_2 = b - r_1q_2$. Donc

$$r_2 = b - r_1q_2 = b - (a - bq_1)q_2 = b - aq_2 + bq_1q_2 = -q_2a + (1 + q_1q_2)b$$

Ce qui matriciellement donne l'expression suivante.

$$\begin{pmatrix} r_1 \\ r_2 \end{pmatrix} = \begin{pmatrix} 1 & -q_1 \\ -q_2 & 1 + q_1q_2 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}$$

Cette matrice s'obtient grâce à la multiplication matricielle suivante.

$$\begin{pmatrix} 0 & 1 \\ 1 & -q_2 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix} = \begin{pmatrix} 1 & -q_1 \\ -q_2 & 1 + q_1q_2 \end{pmatrix}$$

On peut donc utiliser le produit matriciel suivant.

$$\begin{pmatrix} r_1 \\ r_2 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_2 \end{pmatrix} \begin{pmatrix} b \\ r_1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_2 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}$$

1. Le lecteur avancé ne sera pas surpris de ce fait. En effet la multiplication matricielle correspond à la composition d'applications.

Les matrices produits

Maintenant que l'on a vu que des produits matriciels apparaissent, on va apporter une nouvelle notation. Pour chaque $i \in \{1, 2, \ldots, n\}$, on définit la matrice ci-dessous qui est en fait le produit des i premières matrices ayant le quotient comme coefficient.

$$M_i = \begin{pmatrix} s_i & t_i \\ u_i & v_i \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & -q_2 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix}$$

Réécrivons nos étapes sous cette notation. Voici l'étape 1.

$$\begin{pmatrix} b \\ r_1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = M_1 \begin{pmatrix} a \\ b \end{pmatrix}$$

Voici l'étape 2.

$$\begin{pmatrix} r_1 \\ r_2 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_2 \end{pmatrix} \begin{pmatrix} b \\ r_1 \end{pmatrix} = \underbrace{\begin{pmatrix} 0 & 1 \\ 1 & -q_2 \end{pmatrix} M_1}_{M_2} \begin{pmatrix} a \\ b \end{pmatrix} = M_2 \begin{pmatrix} a \\ b \end{pmatrix}$$

Voici l'étape $i+1$

$$\begin{pmatrix} r_i \\ r_{i+1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_{i+1} \end{pmatrix} \begin{pmatrix} r_{i-1} \\ r_i \end{pmatrix} = \underbrace{\begin{pmatrix} 0 & 1 \\ 1 & -q_{i+1} \end{pmatrix} M_i}_{M_{i+1}} \begin{pmatrix} a \\ b \end{pmatrix} = M_{i+1} \begin{pmatrix} a \\ b \end{pmatrix}$$

Et voici l'étape n (la dernière).

$$\begin{pmatrix} \text{pgcd}(a,b) \\ 0 \end{pmatrix} = \begin{pmatrix} r_{n-1} \\ r_n \end{pmatrix} = \underbrace{\begin{pmatrix} 0 & 1 \\ 1 & -q_n \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & -q_2 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix}}_{M_n} \begin{pmatrix} a \\ b \end{pmatrix} = M_n \begin{pmatrix} a \\ b \end{pmatrix}$$

Ainsi, à la dernière étape, on voit la combinaison voulue dans le théorème de Bezout.

$$\begin{pmatrix} \text{pgcd}(a,b) \\ 0 \end{pmatrix} = \begin{pmatrix} r_{n-1} \\ r_n \end{pmatrix} = M_n \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} s_n & t_n \\ u_n & v_n \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} s_n \cdot a & + & t_n \cdot b \\ u_n \cdot a & + & v_n \cdot b \end{pmatrix} \quad (\bigstar)$$

Procédure itérative

Comme on vient de le voir, il faut trouver les coefficients de la matrice M_n pour trouver la combinaison voulue dans le théorème de Bezout.

La méthode la plus simple pour calculer M_n est itérative (penser à une démonstration par récurrence (aussi appelée démonstration par induction)). On connaît la matrice M_1.

$$M_1 = \begin{pmatrix} s_1 & t_1 \\ u_1 & v_1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix} \quad \text{puisque} \quad \begin{pmatrix} b \\ r_1 \end{pmatrix} = M_1 \begin{pmatrix} a \\ b \end{pmatrix}$$

On peut aussi considérer une étape 0 qui fait intervenir une matrice M_0 (qui est l'identité car il s'agit de l'élément neutre de la multiplication).

$$M_0 = \begin{pmatrix} s_0 & t_0 \\ u_0 & v_0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{puisque} \quad \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}$$

Si on connaît la i-ième matrice M_i, on peut trouver la matrice M_{i+1}. En effet, en se basant sur l'étape $i+1$ vue ci-dessus, on voit que :

$$\underbrace{\begin{pmatrix} s_{i+1} & t_{i+1} \\ u_{i+1} & v_{i+1} \end{pmatrix}}_{M_{i+1}} = \begin{pmatrix} 0 & 1 \\ 1 & -q_{i+1} \end{pmatrix} \underbrace{\begin{pmatrix} s_i & t_i \\ u_i & v_i \end{pmatrix}}_{M_i} = \begin{pmatrix} u_i & v_i \\ s_i - u_i q_{i+1} & t_i - v_i q_{i+1} \end{pmatrix}$$

On constate que la première ligne de M_{i+1} est égale à la deuxième ligne de M_i. Il se passe le même phénomène avec les vecteurs issus de l'algorithme d'Euclide.

$$\begin{array}{ccc} \text{Etape } i & \rightsquigarrow & \text{Etape } i+1 \\ M_i = \begin{pmatrix} s_i & t_i \\ u_i & v_i \end{pmatrix} & \rightsquigarrow & \begin{pmatrix} u_i & v_i \\ s_i - u_i q_{i+1} & t_i - v_i q_{i+1} \end{pmatrix} = M_{i+1} \\ \underbrace{\begin{pmatrix} r_{i-1} \\ r_i \end{pmatrix}}_{\text{vecteur de l'étape } i} & \rightsquigarrow & \underbrace{\begin{pmatrix} r_i \\ r_{i+1} \end{pmatrix}}_{\text{vecteur de l'étape } i+1} \end{array}$$

Algorithme

Dans cet algorithme, on place les vecteurs dans la première colonne, les matrices M_i dans les deux colonnes centrales et dans la dernière colonne, on écrit les quotients.

	a	b	
a	1	0	quotients
b	0	1	q_1
$\cdots$	$\cdots$	$\cdots$	$\cdots$
r_{i-1}	s_i	t_i	q_i
r_i	u_i	v_i	q_{i+1}
$r_{i+1} = r_{i-1} - r_i q_{i+1}$	$s_i - u_i q_{i+1}$	$t_i - v_i q_{i+1}$	q_{i+2}
$\cdots$	$\cdots$	$\cdots$	$\cdots$
$r_{n-1} = \text{pgcd}(a,b)$	s_n	t_n	q_n
$r_n = 0$	u_n	v_n	

On trouve à l'avant-dernière ligne la combinaison de Bezout cherchée et un bonus à la dernière ligne (voir formule (★)) : $\text{pgcd}(a,b) = s_n a + t_n b$ et $0 = u_n a + t_n b$.

Remarque

À chaque ligne, on retrouve le terme de gauche en écrivant la combinaison avec les deux termes du milieu.

Quelque soit la ligne, on a $r = s \cdot a + t \cdot b$. Cette propriété permet de repérer une éventuelle erreur de calcul.

Cette propriété est issue des matrices M_i précédentes.
En effet, à chaque étape i, on a bien

$$\begin{pmatrix} r_{i-1} \\ r_i \end{pmatrix} = M_i \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} s_i & t_i \\ u_i & v_i \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} s_i \cdot a & + & t_i \cdot b \\ u_i \cdot a & + & v_i \cdot b \end{pmatrix}$$

	a	b	
a	1	0	quotients
b	0	1	
$\cdots$	$\cdots$	$\cdots$	
r	s	t	
$\cdots$	$\cdots$	$\cdots$	

Proposition 1

Pour tout $i \in \mathbb{N}$, les coefficients de $M_i = \begin{pmatrix} s_i & t_i \\ u_i & v_i \end{pmatrix}$ satisfont la propriété $s_i v_i - t_i u_i = \pm 1$.

Preuve par récurrence

1. Ancrage pour $i = 0$:

   Les coefficients de $M_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ satisfont la propriété qui est : $1 \cdot 1 - 0 \cdot 0 = 1$.

2. Pas de récurrence simple :

   on suppose que c'est vrai pour i et on montre que c'est vrai pour $i+1$.

   L'algorithme d'Euclide étendu dit que :

$$M_{i+1} = \begin{pmatrix} s_{i+1} & t_{i+1} \\ u_{i+1} & v_{i+1} \end{pmatrix} = \begin{pmatrix} u_i & v_i \\ s_i - u_i q_{i+1} & t_i - v_i q_{i+1} \end{pmatrix}$$

   où s_i, t_i, u_i et v_i sont les coefficients de la matrice M_i.

   La propriété peut se simplifier ainsi :

$$\begin{aligned} s_{i+1}v_{i+1} - t_{i+1}u_{i+1} &= u_i(t_i - v_i q_{i+1}) - v_i(s_i - u_i q_{i+1}) \\ &= u_i t_i - v_i s_i = -(s_i v_i - t_i u_i) \overset{\text{HR}}{=} -(\pm 1) = \mp 1 \end{aligned}$$ □

Proposition 2

Soit a et b deux nombres entiers. S'il existe deux nombres entiers x et y tels que

$$ax + by = \pm 1$$

Alors a et b sont premiers entre-eux (c'est-à-dire que $\text{pgcd}(a, b) = 1$).

Preuve

Soit d un diviseur positif de a et de b. Alors d divise ax et by, donc d divise $ax + by$. Comme $ax + by = \pm 1$, on sait donc que d divise ± 1. Or, le seul diviseur positif de ± 1 est 1, donc $d = 1$.

Par conséquent, le seul diviseur positif commun à a et à b est 1. Cela signifie que a et b sont premiers entre-eux. □

Conséquence des propositions 1 et 2

Les nombres qui sont inscrits à chaque ligne dans les colonnes centrales de l'algorithme d'Euclide étendu sont premiers entre-eux !

	a	b	
a	1	0	quotients
b	0	1	q_1
$\cdots$	$\cdots$	$\cdots$	$\cdots$
$r_{n-1} = \text{pgcd}(a, b)$	s_n	t_n	q_n
$r_n = 0$	u_n	v_n	