

Notions réinvesties : théorèmes de Bézout et de Gauss

Une équation diophantienne, en mathématiques, est une équation polynomiale à une ou plusieurs inconnues dont les solutions sont cherchées parmi les nombres entiers, éventuellement rationnels, les coefficients étant eux-mêmes également entiers.

Historiquement, elles sont apparues au III<sup>e</sup> siècle après Jésus-Christ, introduites par le mathématicien grec Diophante d'Alexandrie.

De nombreux problèmes ont depuis lors vu le jour et ont pour certains mis longtemps avant d'être élucidés, comme par exemple le dernier théorème de Fermat caractérisant l'existence de solutions à l'équation  $x^n + y^n = z^n$  en fonction du nombre  $n$ , qui n'a été résolu qu'en 1994 par Andrew Wiles (et Richard Taylor).

## A. Résolution générale

On souhaite résoudre l'équation (E) :  $ax + by = c$  ( $a, b, c$  entiers relatifs avec  $a$  et  $b$  non tous nuls).

### 1. Démontrer que :

si l'équation (E) admet des solutions entières, alors  $c$  est un multiple de  $\text{PGCD}(a; b)$ .

### 2. On supposera par la suite que $c$ est un multiple de $\text{PGCD}(a; b)$ .

a) Démontrer qu'il suffit alors de savoir résoudre une équation du type  $a'x + b'y = c'$  avec  $a'$  et  $b'$  premiers entre eux.

b) Justifier qu'il existe nécessairement une solution à l'équation  $a'x + b'y = c'$ , que l'on note  $(x_0; y_0)$ .

c) Démontrer que si l'équation  $a'x + b'y = c'$  admet une solution  $(x; y)$ , alors  $a' \mid y_0 - y$ .  
En déduire qu'il existe un entier relatif  $k$  tel que  $x = x_0 + b'k$  et  $y = y_0 - a'k$ .

### 3. Conclure quant aux solutions (dans $\mathbb{Z}$ ) de l'équation (E).

## B. Recherche d'une solution particulière : coefficients de Bézout

1. a) Déterminer deux entiers  $u$  et  $v$  tels que  $150u + 31v = 1$ .

b) Déterminer deux entiers  $u$  et  $v$  tels que  $255u + 77v = 1$ .

2. Expliquer pourquoi l'algorithme suivant (en Python) détermine, à partir de l'algorithme d'Euclide, deux entiers  $u$  et  $v$  tels que  $a'u + b'v = 1$  lorsque  $a'$  et  $b'$  sont premiers entre eux :

```
print("Entrez la valeur de a :")
a=int(input())
print("Entrez la valeur de b :")
b=int(input())
r1, u1, v1 = a, 1, 0
r2, u2, v2 = b, 0, 1
print("Voici les coefficients de Bézout en utilisant l'algorithme d'Euclide :")
while r2 != 0:
    q = r1//r2 # quotient de r1 par r2
    rt, ut, vt = r1, u1, v1 # rt = r_temporaire; etc.
    r1, u1, v1 = r2, u2, v2
    r2, u2, v2 = (rt-q*r2), (ut-q*u2), (vt-q*v2)
    print(r2, "=", a, "x", u2, "+", b, "x", v2)
```

3. Écrire un programme en Python qui résout n'importe quelle équation diophantienne  $ax + by = c$ .

## C. Synthèse : méthode générale et exercices

### MÉTHODE DE RÉOLUTION

On note (E) l'équation à résoudre :  $ax + by = c$ .

À savoir (facile à démontrer) :  
si l'équation admet des solutions, alors  $\text{PGCD}(a, b)$  divise  $c$ .

Donc : **Si  $\text{PGCD}(a, b)$  ne divise pas  $c$ , l'équation n'admet pas de solutions.**

**Si  $\text{PGCD}(a, b)$  divise  $c$  :**

**ÉTAPE 1 :** se ramener à une équation avec des entiers premiers entre eux

Diviser l'équation par ce PGCD pour obtenir une équation équivalente du type :

$$(E) \quad a'x + b'y = c'$$

avec  $a'$  et  $b'$  premiers entre eux.

elle existe d'après  
le théorème de Bézout

**ÉTAPE 2 :** recherche d'une solution particulière

Méthode 1 : en testant des entiers simples, déterminer une solution particulière  $(x_0; y_0)$  de (E').

Méthode 2 :

- faire l'algorithme d'Euclide avec  $a'$  et  $b'$
- « remonter » cet algorithme afin de déterminer les coefficients de Bézout pour déterminer une solution particulière de  $a'x + b'y = 1$
- multiplier cette solution particulière par  $c'$  pour en déduire une solution particulière  $(x_0; y_0)$  de (E').

**ÉTAPE 3 :** formes des solutions (avec le théorème de Gauss)

Si (E') admet une solution  $(x; y)$  alors : 
$$\begin{cases} a'x + b'y = c' \\ a'x_0 + b'y_0 = c' \end{cases}$$

Par soustraction, obtenir :  $a'(x - x_0) = b'(y_0 - y)$ .

Donc  $a' \mid b'(y_0 - y)$ .

$a'$  et  $b'$  étant premiers entre eux, utiliser le théorème de Gauss pour obtenir :

$$\exists k \in \mathbb{Z}, x = x_0 + b'k \text{ et } y = y_0 - a'k.$$

**ÉTAPE 4 :** vérification (réciproque)

Vérifier que si  $x = x_0 + b'k$  et  $y = y_0 - a'k$ , avec  $k \in \mathbb{Z}$ , alors ce sont bien des solutions de (E').

**ÉTAPE 5 :** conclusion

Les solutions de (E) sont ...

## EXEMPLE 1

On note (E) l'équation à résoudre :  $600x + 124y = 12$ .

Algorithme d'Euclide pour 600 et 124 :  $600 = 124 \times 4 + 104$

$$124 = 104 \times 1 + 20$$

$$104 = 20 \times 5 + 4$$

$$20 = 4 \times 5 + 0$$

Donc :  $\text{PGCD}(600 ; 124) = 4$ .

### ÉTAPE 1 :

(E)  $\Leftrightarrow \frac{600x + 124y}{4} = \frac{12}{4} \Leftrightarrow 150x + 31y = 3$ . On note (E') cette dernière équation.

Par construction, 150 et 31 sont premiers entre eux. Résoudre (E) revient à résoudre (E').

### ÉTAPE 2 :

Algorithme d'Euclide pour 150 et 31 :  $150 = 31 \times 4 + 26$

$$31 = 26 \times 1 + 5$$

$$26 = 5 \times 5 + 1$$

$$5 = 1 \times 5 + 0$$

Coefficients de Bézout :  $26 = 150 - 31 \times 4$

$$5 = 31 - 26 \times 1$$

$$= 31 - (150 - 31 \times 4) \times 1$$

$$= 150 \times (-1) + 31 \times (1 + 4)$$

$$= 150 \times (-1) + 31 \times 5$$

$$1 = 26 - 5 \times 5$$

$$= 150 - 31 \times 4 - (150 \times (-1) + 31 \times 5) \times 5$$

$$= 150 \times (1 + 5) + 31 \times (-4 - 25)$$

$$= 150 \times 6 + 31 \times (-29)$$

Donc  $(6; -29)$  est une solution particulière de  $150x + 31y = 1$ .

Alors  $(6 \times 3; -29 \times 3)$  ie  $(18; -87)$  est une solution particulière de (E').

### ÉTAPE 3 :

**Si (E') admet une solution**  $(x; y)$  alors : 
$$\begin{cases} 150x + 31y = 3 \\ 150 \times 18 + 31 \times (-87) = 3 \end{cases}$$

Par soustraction :  $150(x - 18) + 31(y + 87) = 0$  donc  $150(x - 18) = 31(-y - 87)$  (\*).

Donc  $150 \mid 31(-y - 87)$ .

Or, 150 et 31 sont premiers entre eux, donc d'après le théorème de Gauss :  $150 \mid -y - 87$ .

D'où :  $\exists k \in \mathbb{Z}$ ,  $-y - 87 = 150k$  ie  $y = -87 - 150k$ .

Alors d'après (\*):  $150(x - 18) = 31 \times 150k$  d'où  $x - 18 = 31k$  ie  $x = 18 + 31k$ .

### ÉTAPE 4 :

**Réciproquement**, si  $x = 18 + 31k$  et  $y = -87 - 150k$  alors :

$150x + 31y = 150(18 + 31k) + 31(-87 - 150k) = 150 \times 18 - 31 \times 87 = 3$  donc  $(x; y)$  est bien une solution de (E').

### ÉTAPE 5 :

**Conclusion :** les solutions de (E) sont les couples  $(18 + 31k; -87 - 150k)$  où  $k \in \mathbb{Z}$ .

## EXEMPLE 2

On note (E) l'équation à résoudre :  $600x + 124y = 10$ .

Algorithme d'Euclide pour 600 et 124 :

- (1)  $600 = 124 \times 4 + 104$
- (2)  $124 = 104 \times 1 + 20$
- (3)  $104 = 20 \times 5 + 4$
- (4)  $20 = 4 \times 5 + 0$

Donc :  $\text{PGCD}(600 ; 124) = 4$ .

Or, 4 ne divise pas 10, donc (E) n'admet aucune solution\*.

\* autre façon de rédiger : supposons par l'absurde que (E) admette des solutions :  $4 \mid 600$  et  $4 \mid 124$  donc, par combinaison linéaire,  $4 \mid 10$ . Or ceci n'est pas le cas, donc notre hypothèse est fautive.

## À VOUS DE JOUER

Résoudre les trois équations diophantiennes suivantes :

$$3x + 7y = 24$$

$$1820x + 858y = 208$$

$$1820x + 585y = 209$$