Arithmétique - Chapitre 4

I. PGCD

I.1. Définitions

Proposition 1. (Définition PGCD)
Soit $(a, b) \in \mathbb{Z}^* \times \mathbb{Z}$.
Il existe un unique **entier naturel** *d, diviseur commun à a et b, tel que l'ensemble des diviseurs communs à a et à b est égal à l'ensemble des diviseurs de d.*
Cet entier naturel est noté $a \wedge b$ et est appelé pgcd de a et b *(plus grand diviseur commun à a et b).*

Démonstration.

- Unicité.
  Soit $(d_1, d_2) \in \mathbb{N}^2$ vérifiant :

$$\left\{\begin{array}{ll} d_1 \mid a, \quad d_1 \mid b & (1) \\ \forall d' \in \mathbb{Z},\ (d' \mid a \ \texttt{ET} \ d' \mid b) \ \Leftrightarrow \ (d' \mid d_1) & (2) \end{array}\right. \quad \text{et} \quad \left\{\begin{array}{ll} d_2 \mid a, \quad d_2 \mid b & (3) \\ \forall d' \in \mathbb{Z},\ (d' \mid a \ \texttt{ET} \ d' \mid b) \ \Leftrightarrow \ (d' \mid d_2) & (4) \end{array}\right.$$

  × Avec (2) et (3), on obtient : $d_2 \mid d_1$.
  × Avec (1) et (4), on obtient : $d_1 \mid d_2$.
  On en déduit : $|d_1| = |d_2|$. Or $(d_1, d_2) \in \mathbb{N}^2$. Ainsi : $d_1 = d_2$.
- Existence. Algorithme d'Euclide.
  On se restreint qu cas où $(a, b) \in \mathbb{N}^* \times \mathbb{N}$ (sinon on se ramène à ce cas en travaillant sur le couple $(|a|, |b|)$. Deux cas se présentent :
  × si $b = 0$, alors, pour tout $n \in \mathbb{N}$:

$$(n \mid a \ \texttt{ET} \ n \mid b) \ \Leftrightarrow \ (n \mid a)$$

  On en déduit : $a \wedge 0 = a$.
  × si $b \neq 0$.
  - On effectue la division euclidienne de a par b.
    On en déduit qu'il existe $(q_1, r_1) \in \mathbb{N}^2$ tel que :

$$\left\{\begin{array}{l} a \ = \ b\,q_1 + r_1 \\ 0 \leqslant r_1 < b \end{array}\right.$$

    On note $Div(a, b)$ l'ensemble des diviseurs communs à a et b. Démontrons : $Div(a, b) = Div(b, r_1)$.
    On porcède par double inclusion.
    $(\subset)$ Soit $n \in Div(a, b)$. Alors :

$$\begin{array}{ll} & n \mid a \ \texttt{ET} \ n \mid b \\ \text{donc} & n \mid bq_1 + r_1 \ \texttt{ET} \ n \mid bq_1 \\ \text{d'où} & n \mid r_1 \ \texttt{ET} \ n \mid b \end{array}$$

    Ainsi : $n \in Div(b, r_1)$.
    $(\supset)$ Soit $n \in Div(b, r_1)$. Alors :

$$\begin{array}{ll} & n \mid b \ \texttt{ET} \ n \mid r_1 \\ \text{donc} & n \mid bq_1 \ \texttt{ET} \ n \mid r_1 \\ \text{d'où} & n \mid b \ \texttt{ET} \ n \mid bq_1 + r_1 \\ \text{ainsi} & n \mid b \ \texttt{ET} \ n \mid a \end{array}$$

    On en déduit : $n \in Div(a, b)$.

- Si $r_1 \neq 0$. On effectue alors la division euclidienne de b par r_1.
  Il existe $(q_2, r_2) \in \mathbb{N}^2$ tel que :
$$\left\{ \begin{array}{l} b \ = \ r_1\, q_2 + r_2 \\ 0 \leqslant r_2 < r_1 \end{array} \right.$$
  Avec la même démonstration que dans le point précédent, on a : $Div(b, r_1) = Div(r_1, r_2)$.
- Si $r_2 \neq 0$, on peut continuer. Il existe $(q_3, r_3) \in \mathbb{N}^2$ tel que :
$$\left\{ \begin{array}{l} r_1 \ = \ r_2\, q_3 + r_3 \\ 0 \leqslant r_3 < r_2 \end{array} \right.$$
  On obtient : $Div(r_1, r_2) = Div(r_2, r_3)$.
- On peut continuer ces divisions tant que le dernier reste n'est pas nul. Mais on ne peut continuer indéfiniment car il n'existe pas de suite $(r_k)_{k \in \mathbb{N}^*}$ strictement décroissante d'entiers (Lemme 1).
  Il existe donc $k_0 \in \mathbb{N}^*$ tel que r_{k_0+1} est le premier reste nul :
$$\begin{array}{rcrcr} a & = & b\, q_1 & + & r_1 \\ b & = & r_1\, q_2 & + & r_2 \\ r_1 & = & r_2\, q_3 & + & r_3 \\ & \vdots & & & \\ r_{k_0-2} & = & r_{k_0-1}\, q_{k_0} & + & r_{k_0} \\ r_{k_0-1} & = & r_{k_0}\, q_{k_0+1} & + & 0 \end{array}$$
  On en déduit :
$$\begin{array}{rcl} Div(a, b) & = & Div(b, r_1) \\ & = & Div(r_1, r_2) \\ & \vdots & \\ & = & Div(r_{k_0-1}, r_{k_0}) \\ & = & Div(r_{k_0}, 0) \ = \ Div(r_{k_0}) \end{array}$$
  où la dernière égalité est obtenue grâce au cas $b = 0$ démontré plus haut).
- On note alors : $a \wedge b = d = r_{k_0}$ et il est caractérisé par la propriété :
$$\forall n \in \mathbb{N}, \quad (n \mid a \ \texttt{ET} \ n \mid b) \ \Leftrightarrow \ (n \mid d)$$

$\square$

Lemme 1.
Il n'existe pas de suite strictement décroissante d'entiers naturels.

Démonstration.
Raisonnons par l'absurde.
Supposons qu'il existe une suite $(r_k)_{k \in \mathbb{N}}$ telle que :

× (r_k) est strictement décroissante,

× $\forall k \in \mathbb{N}, \ r_k \in \mathbb{N}$.

- Tout d'abord, la suite $(r_k)_{k\in\mathbb{N}}$ est :
  × décroissante,
  × minorée par 0.

  Elle converge donc vers un réel ℓ vérifiant : $\ell \geqslant 0$.
- Démontrons maintenant par récurrence : $\forall k \in \mathbb{N}$, $\mathcal{P}(k)$ où $\mathcal{P}(k)$: $r_k \leqslant r_0 - k$.
  - **Initialisation** :
$$r_0 \leqslant \underset{\displaystyle r_0 - 0}{\overset{\displaystyle r_0}{\shortparallel}}$$
    D'où $\mathcal{P}(0)$.
  - **Hérédité** : soit $k \in \mathbb{N}$.
    Supposons $\mathcal{P}(k)$ et démontrons $\mathcal{P}(k+1)$ (*i.e.* $r_{k+1} \leqslant r_0 - (k+1)$).
$$\begin{array}{rrcll} & r_{k+1} & < & r_k & \textit{(car } (r_k) \textit{ strictement décroissante)} \\ \text{donc} & r_{k+1} & \leqslant & r_k - 1 & \textit{(car } r_{k+1} \in \mathbb{N} \textit{ et } r_k \in \mathbb{N}\textit{)} \end{array}$$
    Or, par hypothèse de récurrence : $r_k \leqslant r_0 - k$. D'où : $r_k - 1 \leqslant r_0 - k - 1$. Ainsi, par transitivité :
$$r_{k+1} \leqslant r_k - 1 \leqslant r_0 - (k+1)$$
    D'où $\mathcal{P}(k+1)$.

  Par principe de récurrence : $\forall k \in \mathbb{N}$, $r_k \leqslant r_0 - k$.
- Or : $\lim\limits_{k\to+\infty} r_0 - k = -\infty$.
  Ainsi, par théorème de comparaison : $\lim\limits_{k\to+\infty} r_k = -\infty$.
  Absurde !

□

Exemples

- L'ensemble des diviseurs communs à 12 et 30 est : $Div(12, 30) = \{1, 2, 3, 6\}$.
  Ainsi : $12 \wedge 30 = 6$.
- L'ensemble des diviseurs communs à 27 et 45 est : $Div(27, 45) = \{1, 3, 9\}$.
  Ainsi : $27 \wedge 45 = 9$.

Exercice 1
Déterminer le pgcd de 136 et 472 à l'aide de l'algorithme d'Euclide.

Démonstration.

- On effectue la division euclidienne de 472 par 136.
$$472 = 136 \times 3 + 64$$
- On effectue la division euclidienne de 136 par 64.
$$136 = 64 \times 2 + 8$$
- On effectue la division euclidienne de 64 par 8.
$$64 = 8 \times 9 + 0$$
- D'après l'algorithme d'Euclide, le pgcd de 136 et 472 est le dernier reste non nul obtenu.
  Ainsi : $136 \wedge 472 = 8$.

□

Définition PPCM
Soit $(a, b) \in \mathbb{Z}^2$.
Il existe un unique $m \in \mathbb{N}$ tel que :

1) $a \mid m$ et $b \mid m$,

2) $\forall m' \in \mathbb{N}, \quad (a \mid m' \texttt{ ET } b \mid m') \Leftrightarrow (m \mid m')$.

Cet entier m est appelé *ppcm de a et b* (plus petit multiple commun) et est noté : $a \vee b$.

Exemples

$$4 \vee 6 = 12 \qquad 3 \vee 7 = 21 \qquad 5 \vee 40 = 40 \qquad 7 \vee 18 = 126$$

Commentaire

- Soit $(a, b, c) \in \mathbb{Z}^3$. Par définition du pgcd et du ppcm :
$$\begin{array}{rcl} (a \mid b \texttt{ ET } a \mid c) & \Leftrightarrow & a \mid b \wedge c \\ (b \mid a \texttt{ ET } c \mid a) & \Leftrightarrow & b \vee c \mid a \end{array}$$
- En arithmétique, pour démontrer une égalité, on raisonne souvent par double divisibilité (en prenant garde aux signes).

I.2. Propriétés

Proposition 2.
Soit $(a, b) \in \mathbb{Z}^2$.

1) $a \wedge b = b \wedge a$

2) *Soit $\lambda \in \mathbb{Z}$.* $(\lambda\, a) \wedge (\lambda\, b) = |\lambda|\, (a \wedge b)$.

Démonstration.

1) Immédiat car : $Div(a, b) = Div(b, a)$.

2) Deux cas se présentent :

- si $\lambda = 0$, alors l'égalité : $(\lambda\, a) \wedge (\lambda\, b) = |\lambda|\, (a \wedge b)$ est triviale.
- si $\lambda \neq 0$, on procède par double divisibilité.
  - × Démontrons : $\lambda\, (a \wedge b) \mid (\lambda\, a) \wedge (\lambda\, b)$.
    Par définition de $a \wedge b$: $a \wedge b \mid a$ et $a \wedge b \mid b$. Comme $\lambda \in \mathbb{Z}$:
$$\lambda\, (a \wedge b) \mid \lambda\, a \qquad \text{et} \qquad \lambda\, (a \wedge b) \mid \lambda\, b$$
    Par définition de $(\lambda\, a) \wedge (\lambda\, b)$:
$$\lambda\, (a \wedge b) \mid (\lambda\, a) \wedge (\lambda\, b)$$
  - × Démontrons : $(\lambda\, a) \wedge (\lambda\, b) \mid |\lambda|\, (a \wedge b)$.
    On remarque :
$$\lambda \mid \lambda\, a \qquad \text{et} \qquad \lambda \mid \lambda\, b$$
    On en déduit : $\lambda \mid (\lambda\, a) \wedge (\lambda\, b)$. Il existe donc $r \in \mathbb{Z}$ tel que : $(\lambda\, a) \wedge (\lambda\, b) = r\, \lambda$.
    Or, par définition de $(\lambda\, a) \wedge (\lambda\, b)$:
$$(\lambda\, a) \wedge (\lambda\, b) \mid \lambda\, a \qquad \text{et} \qquad (\lambda\, a) \wedge (\lambda\, b) \mid \lambda\, b$$
    D'où :
$$\lambda\, r \mid \lambda\, a \qquad \text{et} \qquad \lambda\, r \mid \lambda\, b$$

Comme $\lambda \neq 0$:
$$r \mid a \qquad \text{et} \qquad r \mid b$$
Ainsi, par définition de $a \wedge b$: $r \mid a \wedge b$.
D'où : $\lambda\, r \mid \lambda\,(a \wedge b)$, c'est-à-dire :
$$(\lambda\, a) \wedge (\lambda\, b) \mid \lambda\,(a \wedge b)$$

On en déduit :
$$|(\lambda\, a) \wedge (\lambda\, b)| \;=\; |\lambda\,(a \wedge b)| \;=\; |\lambda|\,|a \wedge b|$$
Or un pgcd est positif. D'où : $(\lambda\, a) \wedge (\lambda\, b) \;=\; |\lambda|\,(a \wedge b)$.

□

Proposition 3.
Soit $(a,b) \in \mathbb{Z}^2$.
1) $a \vee b = b \vee a$
2) *Soit* $\lambda \in \mathbb{Z}$. $(\lambda\, a) \vee (\lambda\, b) = |\lambda|\,(a \vee b)$.

Démonstration.
1) Immédiat car les multiples communs à a et b sont évidemment les multiples communs à b et a.
2) Deux cas se présentent :
- si $\lambda = 0$, alors l'égalité à démontrer est triviale.
- si $\lambda \neq 0$, on procède par double divisibilité.
  × Démontrons : $(\lambda\, a) \vee (\lambda\, b) \mid \lambda\,(a \vee b)$.
  Par définition de $a \vee b$:
  $$a \mid a \vee b \qquad \text{et} \qquad b \mid a \vee b$$
  Donc :
  $$\lambda\, a \mid \lambda\,(a \vee b) \qquad \text{et} \qquad \lambda\, b \mid \lambda\,(a \vee b)$$
  Par définition de $(\lambda\, a) \vee (\lambda\, b)$:
  $$(\lambda\, a) \vee (\lambda\, b) \mid \lambda\,(a \vee b)$$
  × Démontrons : $\lambda\,(a \vee b) \mid (\lambda\, a) \vee (\lambda\, b)$.
  On remarque : $\lambda \mid \lambda\, a$. D'où : $\lambda \mid (\lambda\, a) \vee (\lambda\, b)$.
  Ainsi, il existe $r \in \mathbb{Z}$ tel que : $(\lambda\, a) \vee (\lambda\, b) = r\,\lambda$.
  Par définition de $(\lambda\, a) \vee (\lambda\, b)$:
  $$\lambda\, a \mid (\lambda\, a) \vee (\lambda\, b) \qquad \text{et} \qquad \lambda\, b \mid (\lambda\, a) \vee (\lambda\, b)$$
  D'où :
  $$\lambda\, a \mid \lambda\, r \qquad \text{et} \qquad \lambda\, b \mid \lambda\, r$$
  Comme $\lambda \neq 0$:
  $$a \mid r \qquad \text{et} \qquad b \mid r$$
  Par définition de $a \vee b$, on obtient : $a \vee b \mid r$.
  D'où : $\lambda\,(a \vee b) \mid \lambda\, r$, c'est-à-dire :
  $$\lambda\,(a \vee b) \mid (\lambda\, a) \vee (\lambda\, b)$$

On en déduit :
$$|(\lambda\, a) \vee (\lambda\, b)| \;=\; |\lambda\,(a \vee b)| \;=\; |\lambda|\,|a \vee b|$$
Or un ppcm est positif. D'où : $(\lambda\, a) \vee (\lambda\, b) \;=\; |\lambda|\,(a \vee b)$.

□

Proposition 4.
Soit $(a,b) \in \mathbb{Z}^2$. *Soit* $\lambda \in \mathbb{Z}$.

$$a \wedge b \ = \ (a + \lambda\, b) \wedge b$$

Démonstration.
On procède par double divisibilité.

- Démontrons : $a \wedge b \mid (a + \lambda\, b) \wedge b$.
  Par définition de $a \wedge b$, on a :

$$\begin{array}{llcll}
 & a \wedge b \mid a & \texttt{ET} & a \wedge b \mid b & \\
\text{donc} & a \wedge b \mid a & \texttt{ET} & a \wedge b \mid \lambda\, b & \textit{(car } \lambda \in \mathbb{Z}\textit{)} \\
\text{d'où} & a \wedge b \mid (a + \lambda\, b) & \texttt{ET} & a \wedge b \mid b & \\
\text{ainsi} & & a \wedge b \mid (a + \lambda\, b) \wedge b & & \textit{(par définition de } (a + \lambda\, b) \wedge b\textit{)}
\end{array}$$

- Démontrons : $(a + \lambda\, b) \wedge b \mid a \wedge b$.
  On note : $d = (a + \lambda\, b) \wedge b$. Par définition de $(a + \lambda\, b) \wedge b$, on a :

$$\begin{array}{llcll}
 & d \mid (a + \lambda\, b) & \texttt{ET} & d \mid b & \\
\text{donc} & d \mid (a + \lambda\, b) & \texttt{ET} & d \mid \lambda\, b & \textit{(car } \lambda \in \mathbb{Z}\textit{)} \\
\text{d'où} & d \mid a & \texttt{ET} & d \mid b & \\
\text{ainsi} & & \mid a \wedge b & & \textit{(par définition de } a \wedge b\textit{)}
\end{array}$$

Finalement : $|a \wedge b| = |(a + \lambda\, b) \wedge b|$. Or un pgcd est positif. Ainsi :

$$a \wedge b \ = \ (a + \lambda\, b) \wedge b$$

$\square$

Exercice 2
Soit $(a,b) \in \mathbb{Z}^2$.
Calculer $(3a + 7b) \wedge (2a + 5b)$ en fontion de $a \wedge b$.

Démonstration.
On calcule :

$$\begin{array}{rcl}
(3a + 7b) \wedge (2a + 5b) & = & \big((3a + 7b) - (2a + 5b)\big) \wedge (2a + 5b) \\
 & = & (a + 2b) \wedge (2a + 5b) \\
 & = & (a + 2b) \wedge \big((\cancel{2a} + 5b) - 2(\cancel{a} + 2b)\big) \\
 & = & (a + 2b) \wedge b \\
 & = & \big((a + \cancel{2b}) - \cancel{2b}\big) \wedge b \\
 & = & a \wedge b
\end{array}$$

$\square$

I.3. Algorithme d'Euclide en Python

On cherche dans cette partie à coder en **Python** l'algorithme d'Euclide, présenté dans le définition du pgcd.

Commentaire

- Nous avons déjà défini une fonction Descente_Fermat dans le chapitre 1 (Arithmérique - Divisibilité dans $\mathbb{Z}$) permettant d'obtenir le quotient et le reste de la division euclidienne de deux entiers. Cette fonction peut tout à fait être utilisée ici.
- Cependant, nous privilégierons ici la commande prédéfinie en **Python** pour obtenir le reste de la division euclidienne de n par p (où $(n, p) \in \mathbb{Z}^2$). Il s'agit de la commande `n % p`. Par exemple le script :

```
11 % 4
```

renvoie le reste de la division euclidienne de 11 par 4 :

```
3
```

(rappelons que le quotient n'intervient pas dans l'algorithme d'Euclide)

On propose la fonction suivante qui permet d'obtenir le pgcd de deux entiers naturels `a` et `b`.

```
def Algorithme_Euclide(a, b):
    R = [a, b]
    if b > a:
        R = [b, a]
    while (R[0] % R[1]) != 0:
        Aux = R[0]
        R[0] = R[1]
        R[1] = (Aux % R[1])
    return R[1]
```

Détaillons les éléments de ce script.

- **Début de la fonction**

  On commence par préciser la structure de la fonction :

  × cette fonction se nomme `Algorithme_Euclide`,

  × elle prend en entrée les paramètres `a` et `b`,

  × elle admet pour variable de sortie `R[1]`.

```
def Algorithme_Euclide(a, b):
```

```
    return R[1]
```

  On initialise ensuite la variable `R`. Cette variable va contenir, pour chaque division euclidienne à venir :

  - en $1^{\text{ère}}$ coordonnée, le dividende,
  - en $2^{\text{ème}}$ coordonnée, le diviseur.

On choisit donc d'initialiser `R` :

- à `[a, b]` si `a` est supérieur ou égal à `b`,
- à `[b, a]` si `b` est strictement supérieur à `a`.

```
2     if b > a:
3         R = [b, a]
```

- **Structure itérative**
  Les lignes 5 à 8 consistent à déterminer le pgcd de `a` et `b`. Pour cela, on doit déterminer la suite $(r_k)_{k \in \mathbb{N}}$ des restes des divisions euclidiennes de `R[1]` par `R[0]`, jusqu'à trouver un reste nul. Autrement dit, on doit calculer les restes des divisions euclidiennes de `R[1]` par `R[0]` tant qu'on n'obtient un reste non nul. Pour cela, on utilise une structure itérative (boucle while).

```
5     while (R[0] % R[1]) != 0:
```

À chaque tour de boucle, on doit mettre à jour la variable `R`. Pour ce faire, on introduit une variable auxiliaire `Aux`. Détaillons le principe de la mise à jour dans cette boucle while (on se place dans le cas $a \geqslant b$).

× avant le 1er tour de boucle :

`R[0]` contient a et `R[1]` contient b

lors du 1er tour de boucle :

`Aux = R[0]`	(`Aux` contient alors a, valeur contenue dans `R[0]`)
`R[0] = R[1]`	(`R[0]` contient alors b, dernière valeur en date de `R[1]`)
`R[1] = (Aux % R[0])`	(`R[1]` contient alors le reste de la division euclidienne de a par b, dernières valeurs en date de `Aux` et `R[0]` respectivement)

> **Commentaire**
>
> Si on avait réalisé en ligne 8 l'affectation `R[1] = (R[0] % R[1])` alors, on aurait affecté à la variable `R[1]` le reste de la division euclidienne de b (dernière valeur en date de `R[0]`) par b (dernière valeur en date de `R[1]`).

× avant le 2ème tour de boucle, d'après ce qui précède et en notant r_1 le reste de la division euclidienne de a par b :

`R[0]` contient b et `R[1]` contient r_1

lors du 2ème tour de boucle :

`Aux = R[0]`	(`Aux` contient alors b, valeur actuelle de `R[0]`)
`R[0] = R[1]`	(`R[0]` contient alors r_1, dernière valeur en date de `R[1]`)
`R[1] = (Aux % R[0])`	(`R[1]` contient alors le reste de la division euclidienne de b par r_1, dernières valeurs en date de `Aux` et `R[0]` respectivement)

× ...

× avant le $k_0^{\text{ème}}$ tour de boucle, où r_{k_0} est le dernier reste non nul dans l'algorithme d'Euclide (on rappelle qu'on a démontré son existence dans la démonstration) :

$$\texttt{R[0]} \text{ contient } r_{k_0-2} \quad \text{et} \quad \texttt{R[1]} \text{ contient } r_{k_0-1}$$

lors du $k_0^{\text{ème}}$ tour de boucle :

```
Aux = R[0]
```
(`Aux` contient alors r_{k_0-2}, valeur actuelle de `R[0]`)

```
R[0] = R[1]
```
(`R[0]` contient alors r_{k_0-1}, dernière valeur en date de `R[1]`)

```
R[1] = (Aux % R[0])
```
(`R[1]` contient alors le reste de la division euclidienne de r_{k_0-2} par r_{k_0-1}, dernières valeurs en date de `Aux` et `R[0]` respectivement)

À l'issue de ce $k_0^{\text{ème}}$ tour de boucle, le reste de la division euclidienne de r_{k_0-1} (valeur contenue dans `R[0]`) par r_{k_0} (valeur contenue dans `R[1]`) est : $r_{k_0+1} = 0$. La boucle s'arrête donc et renvoie la dernière valeur contenue dans `R[1]`, c'est-à-dire : $r_{k_0} = a \wedge b$.

II. Nombres premiers entre eux

Définition (Nombres premiers entre eux)
Soit $(a, b) \in \mathbb{Z}^2$.
On dit que les entiers a et b sont premiers entre eux si : $a \wedge b = 1$.

⚠ Il ne faut pas confondre « $a \wedge b = 1$ » et « a ne divise pas b ».

Commentaire

Soit $(a, b) \in \mathbb{Z}^2$.
Pour montrer que a et b sont premiers entre eux, il suffit de montrer : $a \wedge b \mid 1$.

Exercice 3
Soit $n \in \mathbb{N}$. Démontrer : $(2^n + 3^n) \wedge (2^{n+1} + 3^{n+1}) = 1$.

Démonstration.
On pose : $d = (2^n + 3^n) \wedge (2^{n+1} + 3^{n+1})$. Par définition de d, on a :

$$d \mid (2^n + 3^n) \quad (1) \qquad\qquad d \mid (2^{n+1} + 3^{n+1}) \quad (2)$$

- On déduit de (1) : $d \mid 3\ (2^n + 3^n)$. D'où : $d \mid (3 \times 2^n + 3^{n+1})$.
  En utilisant (2), on obtient alors :
  $$d \mid \left(3 \times 2^n + \cancel{3^{n+1}} - (2^{n+1} + \cancel{3^{n+1}})\right)$$
  D'où : $d \mid (3 \times 2^n - 2 \times 2^n)$. Ainsi : $d \mid 2^n$.
- De même, en utilisant (1) : $d \mid 2\ (2^n + 3^n)$. D'où : $d \mid (2^{n+1} + 2 \times 3^n)$.
  En utilisant (2), on obtient alors :
  $$d \mid \left(\cancel{2^{n+1}} + 2 \times 3^n - (\cancel{2^{n+1}} + 3^{n+1})\right)$$
  D'où : $d \mid (2 \times 3^n - 3 \times 3^n)$. Ainsi : $d \mid -3^n$. On en déduit : $d \mid 3^n$.

Finalement : $d \mid 2^n \wedge 3^n$.
Or : $2 \wedge 3 = 1$. Donc : $2^n \wedge 3^n = 1$. Ainsi : $d \mid 1$. Finalement : $d = 1$. □

III. Théorème de Bezout

III.1. Écriture du PGCD et théorème de Bezout

Proposition 5.
Soit $(a,b) \in \mathbb{Z}^2$. On note : $d = a \wedge b$.

a) *Il existe $(u,v) \in \mathbb{Z}^2$ tel que : $au + bv = d$.*

b) *Soit $n \in \mathbb{N}$.*

$$\text{Il existe } (u,v) \in \mathbb{Z}^2 \text{ tel que } au + bv = n \quad \Leftrightarrow \quad n \text{ est un multiple de } d$$

Démonstration.

a) On part de l'algorithme d'Euclide, en notant k l'indice du dernier reste non nul.

$$\begin{array}{rcc}
a = bq_1 + r_1 & \text{donc} & a - bq_1 = r_1 \\
b = r_1 q_2 + r_2 & \text{donc} & b - r_1 q_1 = r_2 \\
r_1 = r_2 q_3 + r_3 & \text{donc} & r_1 - r_2 q_3 = r_3 \\
\vdots & & \vdots \\
r_{k-3} = r_{k-2} q_{k-1} + r_{k-1} & \text{donc} & r_{k-3} - r_{k-2} q_{k-1} = r_{k-1} \\
r_{k-2} = r_{k-1} q_k + r_k & \text{donc} & r_{k-2} - r_{k-1} q_k = r_k \\
r_{k-1} = r_k q_{k+1} + 0 & &
\end{array}$$

On obtient alors :

$$\begin{array}{rcll}
d & = & a \wedge b \;=\; r_k & \text{(d'après l'algorithme d'Euclide)} \\
& = & r_{k-2} - r_{k-1} q_k & \\
& = & r_{k-2} - (r_{k-3} - r_{k-2} q_{k-1}) q_k & \\
& = & -q_k r_{k-3} + (q_k q_{k-1} + 1) r_{k-2} & \\
& = & -q_k r_{k-3} + (q_k q_{k-1} + 1)(r_{k-4} - r_{k-3} q_{k-2}) & \\
& = & (q_k q_{k-1} + 1) r_{k-4} - \big(q_k + q_{k-2}(q_k q_{k-1} + 1)\big) r_{k-3} & \\
& \vdots & & \\
& = & au + bv & \text{(où } (u,v) \in \mathbb{Z}^2\text{)}
\end{array}$$

b) On note toujours : $d = a \wedge b$. On procède par double implication.

($\Rightarrow$) Supposons qu'il existe $(u,v) \in \mathbb{Z}^2$ tel que : $n = au + bv$.
Par définition de d, on a : $d \mid a$ et $d \mid b$. Ainsi, comme $(u,v) \in \mathbb{Z}^2$:

$$d \mid au \qquad \text{et} \qquad d \mid bv$$

D'où : $d \mid au + bv$, *i.e.* $d \mid n$.

($\Leftarrow$) Supposons que n est un multiple de d.
Alors il existe $k \in \mathbb{Z}$ tel que : $n = kd$.
D'après le point ***a)***, il existe $(u, v) \in \mathbb{Z}^2$ tel que : $d = au + bv$. D'où :

$$n \; = \; kd \; = \; k\,(au + bv) \; = \; a\,(ku) + b\,(kv) \; = \; au' + bv'$$

Et on a bien : $(u', v') \in \mathbb{Z}^2$.

$\square$

Théorème 1. (Théorème de Bezout)
Soit $(a, b) \in \mathbb{Z}^2$.

$$a \wedge b = 1 \quad \Leftrightarrow \quad \textit{il existe } (u,v) \in \mathbb{Z}^2 \textit{ tel que } au + bv = 1$$

On appelle u *et* v *des* coefficients de Bezout*, ou encore* (u, v) *un* couple de Bezout*.*

⚠ Le couple (u, v) n'est pas unique ! On parle donc d'`UN` couple de Bezout. Par exemple :

$$(-1) \times 2 + 1 \times 3 = 1 \qquad \text{et} \qquad 5 \times 2 + (-3) \times 3 = 1$$

Exercice 4
Calculer le pgcd de 1547 et 632 puis trouver $(u, v) \in \mathbb{Z}^2$ tel que : $1547u + 632v = 1$.

Démonstration.

- On applique l'algorithme d'Euclide.

$$\begin{array}{rcl} 1547 & = & 2 \times 632 + 283 \\ 632 & = & 2 \times 283 + 66 \\ 283 & = & 4 \times 66 + 19 \\ 66 & = & 3 \times 19 + 9 \\ 19 & = & 2 \times 9 + 1 \end{array}$$

  Ainsi : $1547 \wedge 632 = 1$

- De plus :

$$\begin{array}{lrcl} & 283 & = & 1547 - 2 \times 632 \\ \text{donc} & 66 & = & 632 - 2 \times (1547 - 2 \times 632) \; = \; 5 \times 632 - 2 \times 1547 \\ \text{d'où} & 19 & = & (1547 - 2 \times 632) - 4 \times (5 \times 632 - 2 \times 1547) \; = \; 9 \times 1547 - 22 \times 632 \\ \text{ainsi} & 9 & = & (5 \times 632 - 2 \times 1547) - 3 \times (9 \times 1547 - 22 \times 632) \; = \; -29 \times 1547 + 71 \times 632 \\ \text{enfin} & 1 & = & (9 \times 1547 - 22 \times 632) - 2 \times (-29 \times 1547 + 71 \times 632) \; = \; 67 \times 1547 - 164 \times 632 \end{array}$$

  On en conclut, en notant $u = 67$ et $v = -164$:

$$\left\{ \begin{array}{l} (u, v) \in \mathbb{Z}^2 \\ 1547u + 632v \; = \; 1 \end{array} \right.$$

$\square$

Commentaire

Le théorème de Bezout permet de démontrer que 2 nombres sont premiers entre eux.

Exercice 5
Soit $n \in \mathbb{N}$. Démontrer : $(2^n - 1) \wedge (2^{n+1} - 1) = 1$.

Démonstration.
On remarque :
$$-2 \times (2^n - 1) + 1 \times (2^{n+1} - 1) \;=\; 1$$
Or $(-2, 1) \in \mathbb{Z}^2$. Ainsi, par théorème de Bezout : $(2^n - 1) \wedge (2^{n+1} - 1) = 1$. □

III.2. Conséquences du théorème de Bezout

Proposition 6.
Soit $(a, b, c) \in \mathbb{Z}^3$.
$$\left.\begin{array}{l} a \wedge b = 1 \\ a \wedge c = 1 \end{array}\right\} \quad \Rightarrow \quad a \wedge (bc) = 1$$

Démonstration.
- D'après le théorème de Bezout :
  - × Comme $a \wedge b = 1$, il existe $(u_1, v_1) \in \mathbb{Z}^2$ tel que :
  $$a u_1 + b v_1 \;=\; 1$$
  - × Comme $a \wedge c = 1$, il existe $(u_2, v_2) \in \mathbb{Z}^2$ tel que :
  $$a u_2 + c v_2 \;=\; 1$$
- On en déduit :
$$\begin{array}{rcl} 1 & = & (a u_1 + b v_1)\,(a u_2 + c v_2) \\ & = & a^2 u_1 u_2 + a c u_1 v_2 + a b v_1 u_2 + b c v_1 v_2 \\ & = & a \times (a u_1 u_2 + c u_1 v_2 + b v_1 u_2) + bc \times (v_1 v_2) \end{array}$$
  Ainsi, en posant : $u = a u_1 u_2 + c u_1 v_2 + b v_1 u_2$ et $v = v_1 v_2$, on a :
$$\left\{\begin{array}{l} (u, v) \in \mathbb{Z}^2 \\ a\, u + bc\, v = 1 \end{array}\right.$$
  Par théorème de Bezout, on en déduit : $a \wedge (bc) = 1$.

□

Proposition 7. (Généralisations)
1) *Soit* $p \in \mathbb{N}^*$. *Soit* $(a, b_1, b_2, \ldots, b_p) \in \mathbb{Z}^{p+1}$.
$$\left.\begin{array}{c} a \wedge b_1 = 1 \\ a \wedge b_2 = 1 \\ \vdots \\ a \wedge b_p = 1 \end{array}\right\} \quad \Rightarrow \quad a \wedge (b_1 b_2 \cdots b_p) = 1$$

2) *Soit* $(a, b) \in \mathbb{Z}^2$. *Soit* $(k, \ell) \in \mathbb{N}^2$.
$$a \wedge b = 1 \quad \Rightarrow \quad a^\ell \wedge b^k = 1$$

Démonstration.

1) Soit $a \in \mathbb{Z}$. Démontrons par récurrence : $\forall p \in \mathbb{N}^*$, $\mathcal{P}(p)$ où $\mathcal{P}(p)$: $\forall (b_1, \dots, b_p) \in \mathbb{Z}^p$,

$$\left.\begin{array}{c} a \wedge b_1 = 1 \\ a \wedge b_2 = 1 \\ \vdots \\ a \wedge b_p = 1 \end{array}\right\} \quad \Rightarrow \quad a \wedge (b_1 b_2 \cdots b_p) = 1$$

- **Initialisation** : soit $b_1 \in \mathbb{Z}$.
  Supposons $a \wedge b_1 = 1$. Alors : $a \wedge b_1 = 1$.
  D'où $\mathcal{P}(1)$.
- **Hérédité** : soit $p \in \mathbb{N}^*$.
  Supposons $\mathcal{P}(p)$ et démontrons $\mathcal{P}(p+1)$ (*i.e.* $\forall (b_1, \dots, b_p, b_{p+1}) \in \mathbb{Z}^{p+1}$,

  $$\left.\begin{array}{c} a \wedge b_1 = 1 \\ \vdots \\ a \wedge b_p = 1 \\ a \wedge b_{p+1} = 1 \end{array}\right\} \quad \Rightarrow \quad a \wedge (b_1 \cdots b_p \, b_{p+1}) = 1)$$

  Soit $(b_1, \dots, b_p, b_{p+1}) \in \mathbb{Z}^{p+1}$.
  Supposons :

  $$a \wedge b_1 = 1 \qquad \cdots \qquad a \wedge b_p = 1 \qquad a \wedge b_{p+1} = 1$$

  Alors, par hypothèse de récurrence :

  $$a \wedge (b_1 \cdots b_p) = 1 \qquad \text{et} \qquad a \wedge b_{p+1} = 1$$

  Ainsi, par la Proposition 6 appliquée à $b = b_1 \cdots b_p$ et $c = b_{p+1}$, on obtient :

  $$a \wedge (b_1 \cdots b_p \, b_{p+1}) \ = \ 1$$

  D'où $\mathcal{P}(p+1)$.

On conclut par principe de récurrence.

2) • Soit $(a, b) \in \mathbb{Z}^2$.
Supposons : $a \wedge b = 1$.
On commence par démontrer par récurrence : $\forall k \in \mathbb{Z}$, $\mathcal{P}(k)$ où $\mathcal{P}(k)$: $a \wedge b^k = 1$.

- **Initialisation** :
  Par définition du pgcd : $a \wedge b^0 = a \wedge 1 = 1$.
  D'où $\mathcal{P}(0)$.
- **Hérédité** : soit $k \in \mathbb{N}$.
  Supposons $\mathcal{P}(k)$ et démontrons $\mathcal{P}(k+1)$ (*i.e.* $a \wedge b^{k+1} = 1$).
  Par hypothèse de récurrence : $a \wedge b^k = 1$.
  Ainsi, par la Proposition 6 appliquée à $b = b$ et $c = b^k$, on obtient :

  $$a \wedge (b^k \, b) = 1 \qquad i.e. \qquad a \wedge b^{k+1} = 1$$

  D'où $\mathcal{P}(k+1)$.

Par principe de récurrence : $\forall k \in \mathbb{N}$, $a \wedge b^k = 1$. Ainsi :

$$\forall (a, b) \in \mathbb{Z}^2, \quad a \wedge b = 1 \ \Rightarrow \ a \wedge b^k = 1$$

- Soit $(a, b) \in \mathbb{Z}^2$. Soit $(k, \ell) \in \mathbb{N}^2$.
  Supposons : $a \wedge b = 1$.
  × D'après le point précédent : $a \wedge b^k = 1$.
  × On note $c = b^k$. On a alors obtenu : $c \wedge a = a \wedge c = 1$.
  En appliquant encore le point précédent, on obtient : $b \wedge a^\ell = 1$. Ainsi :

$$a^\ell \wedge b^k \; = \; b^k \wedge a^\ell \; = \; c \wedge a^\ell \; = \; 1$$

□

IV. Théorème de Gauss

IV.1. Théorème de Gauss et corollaire

Théorème 2. (Théorème de Gauss)
Soit $(a, b, c) \in \mathbb{Z}^3$.

$$\left.\begin{array}{l} a \mid b\,c \\ a \wedge b \; = \; 1 \end{array}\right\} \quad \Rightarrow \quad a \mid c$$

Démonstration.
Supposons : $a \mid b\,c$ et $a \wedge b = 1$.

- Comme $a \wedge b = 1$, on obtient :

$$c \; = \; c\,(a \wedge b) \; = \; ac \wedge bc$$

- De plus :
  × par hypothèse : $a \mid b\,c$,
  × on a toujours : $a \mid a\,c$.
  On en déduit : $a \mid ac \wedge bc$. D'où : $a \mid c$.

□

Corollaire 1.
Soit $(a, b, c) \in \mathbb{Z}^2$.

$$\left.\begin{array}{l} a \mid c \\ b \mid c \\ a \wedge b \; = \; 1 \end{array}\right\} \quad \Rightarrow \quad a\,b \mid c$$

Démonstration.
Supposons :

$$a \mid c, \qquad b \mid c \qquad \text{et} \qquad a \wedge b = 1$$

- Alors il existe $r \in \mathbb{Z}$ tel que : $c = r\,a$. Ainsi :
  ▸ $b \mid r\,a$
  ▸ $a \wedge b = 1$
  Par théorème de Gauss : $b \mid r$.
- Il existe donc $s \in \mathbb{Z}$ tel que : $r = s\,b$. On en déduit :

$$c \; = \; r\,a \; = \; (s\,b)\,a \; = \; s\,(a\,b)$$

D'où : $a\,b \mid c$.

□

Exercice 6
Soit $n \in \mathbb{N}$. Démontrer que $A = n\,(n^4 - 1)$ est divisible par 10.

Démonstration.

- Comme $10 = 2 \times 5$ et $2 \wedge 5 = 1$, on va démontrer que :
  1) l'entier A est divisible par 2,
  2) l'entier A est divisible par 5.
  En effet, on aura ainsi :
  ▸ $2 \mid A$,
  ▸ $5 \mid A$,
  ▸ $2 \wedge 5 = 1$.
  Par corollaire du théorème de Gauss, on pourra conclure : $10 \mid A$.
- Commençons par démontrer : $2 \mid A$.
  On procède par disjonction de cas.
  × si $n \equiv 0\ [2]$, alors : $2 \mid n$. D'où : $2 \mid n\,(n^4 - 1)$ *i.e.* $2 \mid A$.
  × si $n \equiv 1\ [2]$, alors : $n^4 \equiv 1^4\ [2]$. D'où : $n^4 \equiv 1\ [2]$. Ainsi : $n^4 - 1 \equiv 0\ [2]$.
  On en déduit : $2 \mid (n^4 - 1)$. Donc : $2 \mid n\,(n^4 - 1)$ *i.e.* $2 \mid A$.
- Démontrons enfin : $5 \mid A$.
  On procède encore par disjonction de cas.
  × si $n \equiv 0\ [5]$, alors : $5 \mid n$. D'où : $5 \mid n\,(n^4 - 1)$ *i.e.* $5 \mid A$.
  × si $n \equiv 1\ [5]$, , alors : $n^4 \equiv 1^4\ [5]$. D'où : $n^4 \equiv 1\ [5]$. Ainsi : $n^4 - 1 \equiv 0\ [5]$.
  On en déduit : $5 \mid (n^4 - 1)$. Donc : $5 \mid n\,(n^4 - 1)$ *i.e.* $5 \mid A$.
  × si $n \equiv 2\ [5]$, alors : $n^4 \equiv 16\ [5]$. D'où : $n^4 \equiv 1\ [5]$. Ainsi : $n^4 - 1 \equiv 0\ [5]$.
  Avec le même raisonnement que dans le point précédent, on en déduit : $5 \mid A$.
  × si $n \equiv 3\ [5]$, alors : $n^2 \equiv 9\ [5]$, *i.e.* $n^2 \equiv -1\ [5]$.
  D'où : $n^4 \equiv (-1)^2\ [5]$, *i.e.* $n^4 \equiv 1\ [5]$.
  Avec le même raisonnements que dans les 2 points précédents : $5 \mid A$.
  × si $n \equiv 4\ [5]$, alors : $n^2 \equiv 16\ [5]$, *i.e.* $n^2 \equiv 1\ [5]$.
  D'où : $n^4 \equiv 1^2\ [5]$, *i.e.* $n^4 \equiv 1\ [5]$.
  Avec le même raisonnements que dans les 2 points précédents : $5 \mid A$.

□

IV.2. Conséquences du théorème de Gauss

Proposition 8.
Soit $(a, b) \in \mathbb{Z}^2$. On note : $m = a \vee b$ et $d = a \wedge b$. Alors :

$$|a\,b| \ = \ m\,d$$

Démonstration.

- Par définition de $d = a \wedge b$:
$$d \mid a \qquad \text{et} \qquad d \mid b$$
  Il existe donc $(a', b') \in \mathbb{Z}^2$ tel que : $a = d\,a'$ et $b = d\,b'$.
- De plus :
$$d \ = \ a \wedge b \ = \ (d\,a') \wedge (d\,b') \ = \ d\,a' \wedge b'$$
  Comme $d \neq 0$:
$$a' \wedge b' \ = \ 1$$

- Démontrons alors : $m = d\,a'\,b'$. On procède par double divisibilité.
  - × Démontrons : $m \mid d\,a'\,b'$.
    - Tout d'abord : $a \mid a\,b'$. Donc : $a \mid d\,a'\,b'$.
    - De plus : $b \mid b\,a'$. Donc : $b \mid d\,a'\,b'$.

    Par définition de $m = a \vee b$, on obtient : $m \mid d\,a'\,b'$.
  - × Démontrons : $d\,a'\,b' \mid m$.
    - Tout d'abord, par définition de m, on a :
      $$a \mid m \qquad \text{et} \qquad b \mid m$$
      Ainsi, par définition de $d = a \wedge b$, on obtient : $d \mid m$.
    - Alors il existe $m' \in \mathbb{N}$ tel que : $m = d\,m'$. D'où :
      $$d\,a' \mid d\,n' \qquad \text{et} \qquad d\,b' \mid d\,m'$$
      Comme $d \neq 0$, on en déduit :
      $$a' \mid m' \qquad \text{et} \qquad b' \mid m'$$
    - On obtient alors :
      - ▸ $a' \mid m'$
      - ▸ $b' \mid m'$
      - ▸ $a' \wedge b' = 1$

      Ainsi, par corollaire du théorème de Gauss : $a'\,b' \mid m'$.
      D'où : $d\,a'\,b' \mid d\,m'$, c'est-à-dire :
      $$d\,a'\,b' \mid m$$

    On en déduit : $|m| = |d\,a'\,b'| = |d|\,|a'|\,|b'|$.
    Or les entiers d et m sont positifs. Ainsi : $d\,|a'|\,|b'| = m$.
- On en conclut :
  $$d\,m \;=\; d\,d\,|a'|\,|b'| \;=\; |d\,a'|\,|d\,b'| \;=\; |a|\,|b| \;=\; |a\,b|$$

□

Proposition 9.
Tout rationnel admet un unique représentant irréductible.

Démonstration.

- Existence.
  Soit $r \in \mathbb{Q}$.
  Alors il existe $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$ tel que : $r = \dfrac{a}{b}$.
  - × Par définition de $d = a \wedge b$, on a : $d \mid a$ et $d \mid b$.
    On en déduit qu'il existe $(a', b') \in \mathbb{Z} \times \mathbb{N}^*$ tel que :
    $$a \;=\; d\,a' \qquad \text{et} \qquad b \;=\; d\,b'$$
    On en déduit :
    $$d\,(a' \wedge b') \;=\; (d\,a') \wedge (d\,b') \;=\; a \wedge b$$
  - × De plus, comme $b \neq 0$, alors : $a \wedge b \neq 0$. D'où : $a' \wedge b' = 1$.
  - × Finalement :
    $$\left\{ \begin{array}{l} a' \wedge b' \;=\; 1 \\[2mm] r \;=\; \dfrac{a}{b} \;=\; \dfrac{\cancel{d}\,a'}{\cancel{d}\,b'} \;=\; \dfrac{a'}{b'} \end{array} \right.$$

- Unicité.
  Soit $((a_1, a_2, b_1, b_2) \in \mathbb{Z}^2 \times (\mathbb{N}^*)^2$ tel que :

$$\frac{a_1}{b_1} = \frac{a_2}{b_2}, \qquad a_1 \wedge b_1 = 1 \qquad \text{et} \qquad a_2 \wedge b_2 = 1$$

  En particulier : $a_1\, b_2 = a_2\, b_1$.
  × Comme $b_2 \mid a_1\, b_2$, on en déduit : $b_2 \mid a_2\, b_1$. Ainsi :
    ▸ $b_2 \mid a_2\, b_1$
    ▸ $b_2 \wedge a_2 = 1$
    Par théorème de Gauss, on en déduit : $b_2 \mid b_1$.
  × Comme $b_1 \mid a_2\, b_1$, on en déduit : $b_1 \mid a_1\, b_2$. Ainsi :
    ▸ $b_1 \mid a_1\, b_2$
    ▸ $b_1 \wedge a_1 = 1$
    Par théorème de Gauss, on en déduit : $b_1 \mid b_2$.
  On en déduit : $|b_1| = |b_2|$. Or b_1 et b_2 sont positifs. Donc : $b_1 = b_2$.
  On obtient alors :

$$a_1\, b_2 = a_2\, b_1 = a_2\, b_2$$

  Or $b_2 \neq 0$. D'où : $a_1 = a_2$.

□

Commentaire

On peut retenir que, dès que cela est possible, on travaillera plutôt sur des entiers que sur des rationnels. Il est bien plus simple alors d'exploiter tous les résultats d'arithmétique.

Exercice 7
Démontrer que $\sqrt{2}$ n'est pas rationnel.

Démonstration.
Raisonnons par l'absurde.
Supposons que $\sqrt{2}$ est rationnel.
Il existe donc $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$ tel que :

$$\sqrt{2} = \frac{a}{b} \qquad \text{et} \qquad a \wedge b = 1$$

- On obtient alors : $b\,\sqrt{2} = a$. D'où :

$$b^2\, 2 = a^2$$

  Ainsi : $2 \mid a^2$. D'où : $2 \mid a$ (on peut de nouveau raisonner par l'absurde).
- Il existe alors $p \in \mathbb{Z}$ tel que : $a = 2p$. On en déduit :

$$2\, b^2 = a^2 = (2p)^2 = 4\, p^2$$

  Ainsi : $b^2 = 2\, p^2$. D'où : $2 \mid b^2$. Donc : $2 \mid b$.

Finalement : $2 \mid a \wedge b$.
Absurde ! (car $a \wedge b = 1$.) □

IV.3. Une application : résolution d'équations diophantiennes

Définition (Équation diophantienne)
Soit $(a, b, c) \in \mathbb{Z}^3$.
On appelle *équation diophantienne* toute équation de la forme $ax + by = c$ d'inconnues $(x, y) \in \mathbb{Z}^2$.

Soit $(a, b, c) \in \mathbb{Z}^3$.
Dans toute cette partie, on présente une méthode pour résoudre l'équation diophantienne (E) : $ax+by = c$ (où $(x, y) \in \mathbb{Z}^2$).

1) On vérifie que l'équation (E) admet au moins une solution.

Proposition 10.
Cette équation admet des solutions si et seulement si c est un multiple de $d = a \wedge b$.
En particulier, l'équation $ax + by = 1$ (où $(x, y) \in \mathbb{Z}^2$) admet des solutions si et seulement si $a \wedge b = 1$.

Démonstration.
C'est une reformulation de la Proposition 5. □

2) On cherche une solution particulière à (E).

- Si (E) admet une solution, on a alors :

$$d \mid a, \qquad d \mid b \qquad \text{et} \qquad d \mid c$$

Alors il existe $(a', b', c') \in \mathbb{Z}^3$ tel que :

$$a = da', \qquad b = db' \qquad \text{et} \qquad c = dc'$$

Comme $d = a \wedge b$, alors on a aussi : $a' \wedge b' = 1$.

- On a alors :

$$a\,x + b\,y = c \;\Leftrightarrow\; \cancel{d}a'\,x + \cancel{d}b'\,y = \cancel{d}c' \;\Leftrightarrow\; a'x + b'y = c'$$

- On obtient alors une solution particulière, par exemple, en écrivant l'identité de Bezout :

$$a'u + b'v \;=\; 1$$

(ce qui est possible car : $a' \wedge b' = 1$).
On multiplie ensuite par c'.

Le couple $(x_0, y_0) = (uc', vc') \in \mathbb{Z}^2$ est ainsi une solution particulière de (E).

3) On obtient toutes les solutions à partir d'une solution particulière.
En effet :

$$a'x + b'y = c' \;\Leftrightarrow\; a'x + b'y = a'x_0 + b'y_0 \;\Leftrightarrow\; a'(x - x_0) = -b'(y - y_0)$$

On raisonne alors par analyse-synthèse.

- Analyse.

Soit $(x, y) \in \mathbb{Z}^2$. Supposons que (x, y) est solution de (E). Alors, d'après les équivalences précédentes :

$$a'(x - x_0) = -b'(y - y_0)$$

On en déduit : $a' \mid b'(y - y_0)$. Ainsi :

▸ $a' \mid b'(y - y_0)$,

▸ $a' \wedge b' = 1$.

Par théorème de Gauss, on en déduit : $a' \mid (y - y_0)$. Il existe donc $k \in \mathbb{Z}$ tel que : $y - y_0 = ka'$.

L'équation s'écrit alors :

$$\cancel{a'}(x - x_0) = -b' \times k\,\cancel{a'}$$

$$\text{donc} \qquad x - x_0 = -b'k$$

Finalement :

$$\left\{\begin{array}{lcl} x & = & x_0 - k\,b' \\ y & = & y_0 + k\,a' \end{array}\right.$$

- Synthèse.

  Soit $k \in \mathbb{Z}$. On vérifie que tout couple (x, y) de la forme $(x_0 - kb', y_0 + ka')$ est solution de (E).

  $$\begin{array}{rcll} a'(x_0 - k\,b') + b'(y_0 + k\,a') & = & a'x_0 - \cancel{a'kb'} + b'y_0 + \cancel{b'ka'} & \\ & = & c' & \textit{(car } (x_0, y_0) \textit{ solution de } a'x + b'y = c' \textit{)} \end{array}$$

  On en déduit :

  $$a(x_0 - kb') + b(y_0 + ka') \;=\; da'(x_0 - kb') + db'(y_0 + ka') \;=\; d\left(a'(x_0 - kb') + b'(y_0 + ka')\right) \;=\; d\,c' \;=\; c$$

L'ensemble des solutions de (E) est donc : $\{(x_0 - kb', y_0 + ka') \mid k \in \mathbb{Z}\}$.

Exercice 8

Résoudre dans $\mathbb{Z}^2$ les équations suivantes :

a) $3x - 5y = 0$ ***b)*** $3x - 5y = 12$ ***c)*** $15x - 10y = 7$

Démonstration.

a) On suit la méthode.

1) On remarque : $3 \wedge (-5) = 1$ et $1 \mid 0$. On en déduit que l'équation $3x - 5y = 0$ admet des solutions.

2) Recherche d'une solution particulière.
On remarque :

$$3 \times 5 - 5 \times 3 \;=\; 0$$

Ainsi $(5, 3)$ est une solution particulière de l'équation $3x - 5y = 0$.

3) Obtention de toutes les solutions.
On procède par analyse-synthèse.

- Analyse.

  Soit $(x, y) \in \mathbb{Z}^2$. Supposons que (x, y) est solution de l'équation $3x - 5y = 0$. Alors :

  $$\left\{\begin{array}{rcrcl} 3\,x & - & 5\,y & = & 0 \\ 3 \times 5 & - & 5 \times 3 & = & 0 \end{array}\right.$$

  $$\text{donc} \qquad 3(x - 5) - 5(y - 3) \;=\; 0$$

  $$\text{d'où} \qquad 3(x - 5) \;=\; 5(y - 3)$$

  Or $3 \mid 3(x - 5)$. Ainsi :

  - $3 \mid 5(y - 3)$,
  - $3 \wedge 5 = 1$.

  Par théorème de Gauss : $3 \mid (y - 3)$. On en déduit qu'il existe $K \in \mathbb{Z}$ tel que : $y - 3 = 3K$ *i.e.* $y = 3K + 3$.

Alors :

$$3x - 5(3K+3) = 0$$

$$\text{donc} \qquad \cancel{3}\, x = 5 \times \cancel{3}\,(K+1)$$

$$\text{d'où} \qquad x = 5(K+1)$$

- Synthèse.
  Soit $K \in \mathbb{Z}$. Vérifions que le couple $\big(5(K+1), 3(K+1)\big)$ est solution de l'équation $3x - 5y = 0$.
  $$3 \times 5(K+1) - 5 \times 3(K+1) \ = \ 0$$

Finalement, l'ensemble des solutions de l'équation $3x - 5y = 0$ est :

$$\{\big(5(K+1), 3(K+1)\big) \mid K \in \mathbb{Z}\} \ = \ \{(5k, 3k) \mid k \in \mathbb{Z}\}$$

b) On suit la méthode.

1) On remarque : $3 \wedge (-5) = 1$ et $1 \mid 12$. On en déduit que l'équation $3x - 5y = 12$ admet des solutions.

2) Recherche d'une solution particulière.
On remarque :

$$3 \times 4 - 5 \times 0 \ = \ 12$$

Ainsi $(4, 0)$ est une solution particulière de l'équation $3x - 5y = 12$.

3) Obtention de toutes les solutions.
On procède par analyse-synthèse.

- Analyse.
  Soit $(x, y) \in \mathbb{Z}^2$. Supposons que (x, y) est solution de l'équation $3x - 5y = 12$. Alors :
  $$\left\{\begin{array}{rcrcl} 3\,x & - & 5\,y & = & 12 \\ 3 \times 4 & - & 5 \times 0 & = & 12 \end{array}\right.$$
  $$\text{donc} \qquad 3(x-4) - 5(y-0) \ = \ 0$$
  $$\text{d'où} \qquad 3(x-4) \ = \ 5y$$
  Or $3 \mid 3(x-4)$. Ainsi :
  - $3 \mid 5y$,
  - $3 \wedge 5 = 1$.

  Par théorème de Gauss : $3 \mid y$. On en déduit qu'il existe $k \in \mathbb{Z}$ tel que : $y = 3k$. Alors :
  $$3x - 5 \times 3k = 12$$
  $$\text{donc} \qquad \cancel{3}\, x = \cancel{3}\,(5k+4)$$
  $$\text{d'où} \qquad x = 5k + 4$$
- Synthèse.
  Soit $k \in \mathbb{Z}$. Vérifions que le couple $(5k+4, 3k)$ est solution de l'équation $3x - 5y = 12$.
  $$3 \times (5k+4) - 5 \times 3k \ = \ \cancel{15k} + 12 - \cancel{15k} \ = \ 12$$

Finalement, l'ensemble des solutions de l'équation $3x - 5y = 12$ est :

$$\{(5k+4, 3k) \mid k \in \mathbb{Z}\}$$

c) On suit la méthode.

1) On remarque : $15 \wedge (-10) = 5$ et $5 \nmid 7$. On en déduit que l'équation $15x - 10y = 7$ n'admet pas de solutions.

□