Chapitre 5

Plus grand commun diviseur

Sommaire

Sauf indication contraire, dans tout le chapitre, on ne considèrera que des nombres entiers positifs et leurs diviseurs positifs.

Trois axiomes [1] fondamentaux de l'arithmétique, dont nous aurons besoin dans ce chapitre :

Axiome 1 : Toute partie non vide de $\mathbb{N}$ admet un plus petit élément (c'est faux dans $\mathbb{Z}$).

Axiome 2 : Toute partie non vide et majorée de $\mathbb{N}$ admet un plus grand élément.

Axiome 3 : Toute suite d'entiers naturels strictement décroissante est finie (c'est faux dans $\mathbb{Z}$).

1. Un axiome désigne une vérité première – donc qui ne se démontre pas – à l'intérieur d'une théorie.

5.1 Diviseurs communs à deux entiers naturels – PGCD

5.1.1 Définitions

Définition 5.1. $\forall (a\,;\,b) \in \mathbb{N}^2$. On notera :
- $\mathscr{D}(a)$ l'ensemble des diviseurs positifs de a ;
- $\mathscr{D}(a,b) = \mathscr{D}(b,a) = \mathscr{D}(a) \cap \mathscr{D}(b)$ l'ensemble des diviseurs positifs communs à a et à b

$\forall (a\,;\,b) \in \mathbb{N}^2$, ces deux ensembles sont non vides : 1 divisant tout nombre, il appartient à $\mathscr{D}(a)$ et à $\mathscr{D}(b)$ et donc aussi à $\mathscr{D}(a,b)$
Tout élément de $\mathscr{D}(a)$ est inférieur à a donc $\mathscr{D}(a)$ est un ensemble non vide et majoré : il admet donc un plus grand élément (axiome 2). On le savait : il s'agit de a. Mais il en va de même de $\mathscr{D}(a,b)$: c'est un ensemble non vide car il contient 1 ; il est majoré par a ou b car tout diviseur de a est inférieur à a et tout diviseur de b est inférieur à b donc tout diviseur de a et de b est inférieur au minimum de a et de b. Il admet donc un plus grand élément.

Définition 5.2. On appelle *plus grand commun diviseur* de a et b le plus grand élément de $\mathscr{D}(a,b)$. On le note PGCD(a,b) ou $a \wedge b$.

Définition 5.3. Deux entiers naturels a et b sont dits *premiers entre eux* si $a \wedge b = 1$.

5.1.2 Premières propriétés

Propriété 5.1. *Soit c un entier naturel quelconque. L'ensemble des diviseurs communs entre c et 0 est égal à l'ensemble des diviseurs de c.*

$$\forall c \in \mathbb{N}, \quad \mathscr{D}(c,0) = \mathscr{D}(c)$$

Preuve. $\mathscr{D}(0) = \mathbb{N}^*$ car tout entier naturel non nul divise 0 et, comme 0 ne divise aucun nombre, $\forall c \in \mathbb{N}$, $0 \notin \mathscr{D}(c)$. Donc $\forall c \in \mathbb{N}$, $\mathscr{D}(c,0) = \mathscr{D}(c) \cap \mathbb{N}^* = \mathscr{D}(c)$. ♢

Propriété 5.2. *Soit a et b deux entiers naturels quelconques. Si b divise a alors le plus grand commun diviseur de a et b est b.*

$$\forall (a,b) \in \mathbb{N}^2, \quad b \mid a \Rightarrow a \wedge b = b$$

Preuve. $b \mid a \Rightarrow b \in \mathscr{D}(a)$. De plus $b \mid a \Rightarrow b \leqslant a$. Par ailleurs $b \in \mathscr{D}(b)$ donc $b \in \mathscr{D}(a,b)$. On a vu que tout élément de $\mathscr{D}(a,b)$ est inférieur au minimum de a et de b, ici b. Donc b est le plus grand élément de $\mathscr{D}(a,b)$, donc $a \wedge b = b$. ♢

Propriété 5.3. *Soit a et b deux entiers naturels tels que $b < a$. L'ensemble des diviseurs de a et b est égal à l'ensemble des diviseurs de b et $a - b$.*

$$\forall (a,b) \in \mathbb{N} \text{ tels que } a < b, \quad \mathscr{D}(a,b) = \mathscr{D}(b, a-b)$$

Preuve. $n \in \mathscr{D}(a,b) \Leftrightarrow n \in \mathscr{D}(a) \cap \mathscr{D}(b) \Leftrightarrow n \mid a$ et $n \mid b \Rightarrow n$ divise toute combinaison linéaire de a et de b, en particulier $a - b (> 0) \Rightarrow n \in \mathscr{D}(b) \cap \mathscr{D}(a-b) = \mathscr{D}(b, a-b)$.
On vient de démontrer que $n \in \mathscr{D}(a,b) \Rightarrow n \in \mathscr{D}(b,a-b)$, c'est-à-dire que $\mathscr{D}(a,b) \subset \mathscr{D}(b,a-b)$.

$n \in \mathscr{D}(b,a-b) \Leftrightarrow n \in \mathscr{D}(b) \cap \mathscr{D}(a-b) \Leftrightarrow n \mid b$ et $n \mid a-b \Rightarrow n$ divise toute combinaison linéaire de b et de $a-b$, en particulier $b + (a-b) = a \Rightarrow n \in \mathscr{D}(a) \cap \mathscr{D}(b) = \mathscr{D}(a,b)$.
On vient de démontrer que $n \in \mathscr{D}(b,a-b) \Rightarrow n \in \mathscr{D}(a,b)$, c'est-à-dire que $\mathscr{D}(b,a-b) \subset \mathscr{D}(a,b)$.

On a donc $\mathscr{D}(a,b) \subset \mathscr{D}(b,a-b)$ et $\mathscr{D}(b,a-b) \subset \mathscr{D}(a,b)$, donc $\mathscr{D}(b,a-b) = \mathscr{D}(a,b)$.

♢

5.1.3 Recherche du PGCD : Algorithme d'EUCLIDE

Propriété 5.4. *Soit deux entiers naturels a et b avec $a > b$ et l'unique couple d'entiers (q, r) tels que $a = bq + r$ avec $0 \leqslant r < b$. Alors l'ensemble des diviseurs de a et de b est l'ensemble des diviseurs de b et de r.*

$$\forall (a, b, q, r) \in \mathbb{N}^4 \text{ tels que } a > b \text{ et } a = bq + r \text{ avec } 0 \leqslant r < b \Rightarrow \mathscr{D}(a, b) = \mathscr{D}(b, r)$$

Preuve. Comme vu dans la précédente preuve, $n \in \mathscr{D}(a, b) \Rightarrow n$ divise toute combinaison linéaire de a et de b, en particulier $a - bq = r \Rightarrow n \in \mathscr{D}(b, r)$ donc $\mathscr{D}(a, b) \subset \mathscr{D}(b, r)$.
$n \in \mathscr{D}(b, r) \Rightarrow n$ divise toute combinaison linéaire de b et de r, en particulier $bq + r = a \Rightarrow n \in \mathscr{D}(a, b)$ donc $\mathscr{D}(b, r) \subset \mathscr{D}(a, b)$.
On a donc $\mathscr{D}(a, b) \subset \mathscr{D}(b, r)$ et $\mathscr{D}(b, r) \subset \mathscr{D}(a, b)$, donc $\mathscr{D}(a, b) = \mathscr{D}(b, r)$. ♢

Principe de l'algorithme d'EUCLIDE

On cherche à déterminer le PGCD de deux nombres positifs a et b (avec $a > b$).
- Si $b \mid a$ alors $a \wedge b = b$
- Sinon on applique l'algorithme suivant :
  - $\mathscr{D}(a, b) = \mathscr{D}(b, r)$ avec $a > b > r$
  - Comme on a supposé que b ne divise pas a, alors $r \neq 0$ et $\mathscr{D}(b, r) = \mathscr{D}(r, r_1)$ où r_1 est le reste de la division de b par r donc $r > r_1$
  - Si $r_1 \neq 0$ alors $\mathscr{D}(r, r_1) = \mathscr{D}(r_1, r_2)$ où r_2 est le reste de la division de r par r_1 donc $r_1 > r_2$

La suite des restes successifs est un suite d'entiers naturels strictement décroissante, elle est donc finie (axiome 3).
L'un des restes finira par être nul et, à un certain rang n, on aura :

$$\mathscr{D}(a, b) = \mathscr{D}(b, r) = \mathscr{D}(r, r_1) = \mathscr{D}(r_1, r_2) = \ldots = \mathscr{D}(r_n, 0) = \mathscr{D}(r_n)$$

Le PGCD de a et b est donc le plus grand diviseur de r_n, c'est-à-dire r_n lui-même.
Finalement : Lorsque b ne divise pas a, le PGCD de a et b est le dernier reste non nul obtenu par l'algorithme d'EUCLIDE.

5.1.4 Premières propriétés du PGCD

Une conséquence de la preuve est la propriété suivante :

Propriété 5.5. *Soit deux entiers naturels a et b et g leur PGCD. L'ensemble des diviseurs de a et b est l'ensemble des diviseurs de g.*

$$\forall (a, b) \in \mathbb{N}^2, a \wedge b = g \Rightarrow \mathscr{D}(a, b) = \mathscr{D}(g)$$

Propriété 5.6. *Soit a, b deux entiers naturels dont un au moins est non nul et k un entier naturel.* PGCD(ka, kb) = kPGCD(a, b).

$$\forall (a, b) \in \mathbb{N}^2, (a, b) \neq (0, 0), \forall k \in \mathbb{N}^*, ka \wedge kb = k(a \wedge b)$$

Preuve.
- Si a ou b est nul, par exemple b, on a vu que $a \wedge 0 = a$ et donc $ka \wedge k \times 0 = ka \wedge 0 = ka = k(a \wedge 0)$.
- Si $b \mid a$, on a vu que $a \wedge b = b$. Par ailleurs, si $b \mid a$ alors $kb \mid ka$ et de la même manière $ka \wedge kb = kb$. On a donc $ka \wedge kb = k(a \wedge b)$.

- Sinon, en supposant que $a > b$ et que $a = bq + r$ avec $0 < r < b$, on a alors $ka = kbq + kr$ avec $0 < kr < kb$. Comme vu dans l'algorithme d'Euclide, au même rang n, nous aurons :

$$\mathscr{D}(ka, kb) = \mathscr{D}(kb, kr) = \mathscr{D}(kr, kr_1) = \mathscr{D}(kr_1, kr_2) = \ldots = \mathscr{D}(kr_n, 0) = \mathscr{D}(kr_n)$$

  Et donc $ka \wedge kb = kr_n = k(a \wedge b)$.

$\diamondsuit$

Propriété 5.7. *Soit deux entiers naturels a et b. g est le PGCD de a et b si et seulement si g divise a, g divise b et les entiers $a' = \frac{a}{g}$ et $b' = \frac{b}{g}$ sont premiers entre eux.*

Preuve.

⇒ : Supposons $g = a \wedge b$ donc par définition $a = ga'$ et $b = gb'$. $g = a \wedge b = ga' \wedge gb' = g(a' \wedge b')$ donc $a' \wedge b' = 1$.

⇐ : Soit un diviseur g de a et b tel que $a' \wedge b' = 1$. Alors $a \wedge b = ga' \wedge gb' = g(a' \wedge b') = g$.

$\diamondsuit$

5.2 Théorèmes et applications

5.2.1 Théorème de BÉZOUT

Propriété 5.8 (Identité de BÉZOUT)**.** $\forall (a, b) \in \mathbb{N}^2$, $a \wedge b = g \Rightarrow \exists (u, v) \in \mathbb{Z}^2 / au + bv = g$.

Remarque. La réciproque de l'identité de BÉZOUT est fausse : $3 \times 2 - 2 \times 2 = 2$ mais $3 \wedge 2 \neq 2$.

Exemple 5.1. $390 \wedge 104 = 26$ donc on sait qu'il existe au moins un couple d'entiers (u, v) tel que $390u + 104v = 26$.
Comment trouver un tel couple ?

- On peut tatonner. Par exemple en passant par le tableau de valeurs de la fonction $v \longmapsto u = \frac{26-104v}{390}$ jusqu'à trouver un couple où u et v sont entiers. On finit par trouver $(u, v) = (-1; 4)$, par exemple, ou bien $(u, v) = (-5; 19)$.
- On peut « remonter » l'algorithme d'EUCLIDE :

Algorithme d'EUCLIDE :

$$\begin{aligned} 390 &= 3 \times 104 + 78 \\ 104 &= 1 \times 78 + 26 \\ 78 &= 3 \times 26 + 0 \end{aligned}$$

Donc 26 est le PGCD et :

$$\begin{aligned} 26 &= 104 - 1 \times 78 \\ 26 &= 104 - 1 \times (390 - 3 \times 104) \\ &= 4 \times 104 - 1 \times 390 \end{aligned}$$

Preuve. Prouvons l'identité de BÉZOUT.

- Soit $\mathscr{E}$ l'ensemble des nombres entiers naturels non nuls tels que $au + bv$, avec u et v entiers relatifs.
  $a = 1a + 0b$ donc $a \in \mathscr{E} \neq \varnothing$. Donc $\mathscr{E}$ contient un plus petit élément (axiome 1). Appelons-le e.
- Soit $g = a \wedge b$. Comme g divise a et b, alors g divise e.
- Soit (q, r) issus de la division euclidienne de a par e : $a = eq + r$ où $0 \leqslant r < e$.
  $r = a - eq$ donc r est une combinaison linéaire de a et de e par conséquent c'est aussi une combinaison linéaire de a et de b. Si $r > 0$ alors $r \in \mathscr{E}$ mais comme $r < e$ on a une contradiction car e est le plus petit élément de $\mathscr{E}$. Donc $r = 0$, $a = eq$ et e divise a.
  On démontre de la même manière que e divise b.
  e divise a et b donc e divise g.

- Comme $e \mid g$ et $g \mid e$ alors $g = e$.
  Donc $g \in \mathscr{E}$, donc il existe un couple (u, v) tel que $g = au + bv$.

$\diamondsuit$

Théorème 5.9 (Théorème de Bézout)**.** *Deux entiers naturels a et b sont premiers entre eux si et seulement si il existe deux entiers relatifs u et v tels que $au + bv = 1$.*

$$\forall (a, b) \in \mathbb{N}^2, \quad a \wedge b = 1 \Leftrightarrow \exists (u, v) \in \mathbb{Z}^2 / au + bv = 1$$

Preuve.

$\Rightarrow$: C'est une simple application de l'identité de Bézout.

$\Leftarrow$: $\exists (u, v) \in \mathbb{Z}^2 / au + bv = 1$. Soit $g = a \wedge b$. $g \mid a$ et $g \mid b$ donc $g \mid au + bv = 1$ donc $g = 1$.

$\diamondsuit$

Exemple. $\forall n \in \mathbb{N}^*$, $3(5n+7) - 5(3n+4) = 1$ donc $(5n+7) \wedge (3n+4) = 1$.

5.2.2 Théorème de Gauss

Théorème 5.10 (Théorème de Gauss)**.** *Soit a, b et c trois entiers naturels. Si a divise bc et si a est premier avec b, alors a divise c.*

$$\forall (a, b, c) \in \mathbb{N}^3, \quad a \mid bc \text{ et } a \wedge b = 1 \Rightarrow a \mid c$$

La réciproque est fausse.

Preuve. $a \mid bc \Leftrightarrow \exists q \in \mathbb{N} / bc = aq$.
$a \wedge b = 1$ donc, d'après Bézout, $\exists (u, v) \in \mathbb{Z}^2 / au + bv = 1 \Rightarrow auc + bvc = c \Leftrightarrow auc + avq = c \Leftrightarrow a\underbrace{(uc + vq)}_{\in \mathbb{Z}} = c \Rightarrow a \mid c$. $\diamondsuit$

Corollaire 5.11. *Si un entier c est divisible par des entiers a et b premiers entre eux, alors c est divisble par leur produit ab.*

Preuve. $a \mid c$, $b \mid c$ et $a \wedge b = 1$.
$\exists (k, k') \in \mathbb{Z}^2 / c = ak$ et $c = bk'$ donc $ak = bk'$ et $a \mid bk'$. D'après Gauss, comme $a \wedge b = 1$ alors $a \mid k'$ donc $\exists k'' \in \mathbb{Z} / ak'' = k' \Leftrightarrow c = bk' = abk''$ donc $ab \mid c$. $\diamondsuit$

Corollaire 5.12. *Si un entier premier divise un produit de facteurs alors il divise au moins l'un des facteurs.*

Preuve. Soit p premier et divisant le produit de facteurs ab.
Si $p \mid a$ alors p divise au moins a.
Sinon, comme p est premier, $p \wedge a = 1$ donc, Gauss, $p \mid b$. $\diamondsuit$

Corollaire 5.13. *Si un entier premier divise un produit de facteurs premiers, alors il est égal à l'un d'entre eux.*

Preuve. Soit a, b et p premiers tels que $p \mid ab$.
Si $p \mid a$, comme a et p premiers, alors $a = p$.
Sinon, Gauss, $p \mid b$ et, comme p et b premiers, alors $b = p$. $\diamondsuit$

Corollaire 5.14. *Un entier p est premier avec a et b si et seulement si il est premier avec leur produit ab.*

Preuve.

⇒ : Supposons $p \wedge a = 1$ et $p \wedge b = 1$.
Soit $d \in \mathscr{D}(p, ab)$. Alors ($d \mid p$ et $d \mid ab$) donc ($d \mid ap$ et $d \mid ab$) donc $d \mid ap \wedge ab = a(p \wedge b) = a \times 1 = a$ mais $d \mid p$ donc $d \mid a \wedge p = 1$ donc $d = 1$.
Ainsi, $\forall d \in \mathscr{D}(p, ab)$, $d = 1$ donc p et ab sont premiers entre eux.

⇐ : Supposons $p \wedge ab = 1$.
Soit $d \in \mathscr{D}(p, a)$. ($d \mid p$ et $d \mid a$) donc ($d \mid p$ et $d \mid ab$) donc $d \mid p \wedge ab = 1$ donc $d = 1$.
Ainsi, $\forall d \in \mathscr{D}(p, a)$, $d = 1$ donc p et a sont premiers entre eux.
On démontre de la même manière que p et b sont premiers entre eux.

♢

5.2.3 Application : Résolution d'équations diophantiennes

Définition 5.4. Soit a et b deux entiers non nuls et c un entier quelconque. Une *équation diaphantienne* est une équation de la forme $ax + by = c$, d'inconnues entières x et y.
Résoudre une telle équation c'est trouver *tous* les couples d'entiers vérifiant l'équation.

Lorsque $c = a \wedge b$: On a déjà vu qu'il existe au moins une solution (BÉZOUT) et, dans l'exemple 5.1 en appliquant l'algorithme d'EUCLIDE puis en le « remontant », on sait obtenir cette solution particulière : $390x + 104y = 26$ admet comme solution particulière le couple $(x, y) = (-1; 4)$ car $390 \times (-1) + 104 \times 4 = 26$.

$$\begin{aligned} 390x + 104y &= 26 && (L_1)\\ 390 \times (-1) + 104 \times 4 &= 26 && (L_2)\\ 390(x+1) + 104(y-4) &= 0 && (L_1 - L_2) \end{aligned}$$

Ainsi $390(x+1) = 104(-y+4)$ et, en divisant par $390 \wedge 104 = 26$, $15(x+1) = 4(-y+4)$ et les coefficients 15 et 4 sont premiers entre eux.
Donc, GAUSS, $15 \mid -y + 4 \Leftrightarrow y = 4 - 15k$ avec $k \in \mathbb{Z}$.
On a alors $15(x+1) = 4(-4 + 15k + 4) \Leftrightarrow 15(x+1) = 4 \times 15k \Leftrightarrow x = -1 + 4k$ avec $k \in \mathbb{Z}$.
Comme il s'agit du même entier k, pour chaque valeur de k, on obtient un couple unique (x, y) solution de l'équation diophantienne $390x + 104y = 26$ et l'ensemble des solutions de l'équation est $\mathscr{S} = \{(-1 + 4k; 4 - 15k), k \in \mathbb{Z}\}$.

Lorsque c est un multiple de $a \wedge b$: Par exemple $390x + 104y = 52 = 2(390 \wedge 104)$.
On trouve une solution particulière de $390x + 104y = 390 \wedge 104$ qui existe forcément. On obtient $390 \times (-1) + 104 \times 4 = 26 \Leftrightarrow 390 \times (-2) + 104 \times 8 = 52$.

$$\begin{aligned} 390x + 104y &= 52 && (L_1)\\ 390 \times (-2) + 104 \times 8 &= 52 && (L_2)\\ 390(x+2) + 104(y-8) &= 0 && (L_1 - L_2) \end{aligned}$$

On divise par $390 \wedge 104 = 26$ et, à l'aide de GAUSS, on obtient de la même manière l'ensemble des solutions : $\mathscr{S} = \{(-2 + 4k, 8 - 15k), k \in \mathbb{Z}\}$.

Lorsque c n'est pas un multiple de $a \wedge b$: L'équation n'a pas de solution (la preuve en est laissée pour l'exercice 5.16).

5.3 Exercices

5.3.1 PGCD

EXERCICE 5.1.
Déterminer, à l'aide de l'algorithme d'EUCLIDE, les PGCDs suivants :

- $279 \wedge 11\,222$
- $181 \wedge 1\,027$
- $747 \wedge 310$
- $6\,157 \wedge 1\,645$
- $2\,002 \wedge 2\,015$
- $147 \wedge 741$

EXERCICE 5.2.
Soit $n \in \mathbb{N}$. $a = n+3$ et $b = 2n+1$. On pose $g = a \wedge b$.

1. Montrer que $g \in \mathscr{D}(5)$.
2. En déduire pour quelle(s) valeur(s) de n on a $g = 5$ et pour quelle(s) valeur(s) de n on a $g = 1$.

EXERCICE 5.3.
On pose $a = 630$ et $b \in \mathbb{N}$. Sachant que $a \wedge b = 105$ et que $600 < b < 1\,100$ déterminer b.

EXERCICE 5.4.
Si on divise 2 897 et 3 505 par un même entier positif on obtient, respectivement, 13 et 5 comme restes. Quel est cet entier ?

EXERCICE 5.5.
Calculer, en utilisant l'algorithme d'EUCLIDE, $2^{12} - 1 \wedge 2^{21} - 1$.

EXERCICE 5.6.
Quel est le PGCD de :

1. deux entiers consécutifs ?
2. deux entiers pairs consécutifs ?
3. deux entiers impairs consécutifs ?

EXERCICE 5.7.
Soit n un entier naturel. Déterminer $A \wedge B$ dans chacun des cas suivants :

1. $A = 3n^2 + n$ et $B = 3n^2$
2. $A = 3n^2 + 2n$ et $B = 2n^2 + n$

EXERCICE 5.8.
Pour tout entier naturel n, on définit $a = 4n+1$ et $b = 5n+3$.
On s'intéresse aux valeurs du PGCD de a et b en fonction de n.

1. Recherche d'une conjecture avec un logiciel
   (a) Sur un tableur, créer 3 colonnes donnant les valeurs de n, a et b pour n variant de 0 à 100, puis une quatrième avec les valeurs de $a \wedge b$.
   (b) Quelles semblent être les valeurs possibles de ce PGCD ?
   (c) Conjecturer la caractéristique des nombres n tels que le PGCD soit différent de 1.
2. Démonstrations
   (a) Démontrer la conjecture faite au 1b.
   (b) En raisonnant par disjonction des cas, déterminer les valeurs de n telles que $a \wedge b = 7$.

EXERCICE 5.9.
Déterminer les couples d'entiers naturels (a, b) dans chacun des cas suivants :

1. $a + b = 72$ et $a \wedge b = 9$
2. $a \times b = 439\,230$ et $a \wedge b = 121$
3. $a^2 - b^2 = 5\,440$ et $a \wedge b = 8$

EXERCICE 5.10.
Soit a et b deux entiers naturels non nuls.

1. Démontrer que si $\frac{3a+4b}{5a+7b}$ est irréductible, il en est de même de la fraction $\frac{a}{b}$.
2. Inversement démontrer que si $\frac{3a+4b}{5a+7b}$ n'est pas irréductible, il en est de même de la fraction $\frac{a}{b}$.

5.3.2 Applications des théorèmes

EXERCICE 5.11.
Montrer que $\forall n \in \mathbb{N}$, $n^3 - n$ est divisible par 6.

EXERCICE 5.12.
En trouvant à chaque fois une combinaison linéaire adaptée, démontrer que les entiers u et v suivants sont premiers entre eux :

1. $u = -n+4$ et $v = 3n-11$
2. $u = 6n+3$ et $v = 3n+1$
3. $u = 2n-1$ et $v = -7n+3$

EXERCICE 5.13.
Résoudre dans $\mathbb{Z}$ les équations suivantes :

1. $7x = 11y$
2. $63n = 91n$
3. $208a = 390b$

EXERCICE 5.14.
Déterminer tous les entiers n tels que, quand on divise n par 60 et par 156, le reste soit égal à 15.

EXERCICE 5.15.
Trouver les entiers a et b tels que $a \wedge b = 21$ et vérifiant $99a - 165b = 0$.

5.3.3 Équations diophantiennes

EXERCICE 5.16.
Montrer qu'une équation diophantienne $ax + by = c$ n'a pas de solution quand c n'est pas un multiple de $a \wedge b$.

EXERCICE 5.17.
Sans les résoudre, déterminer si les équations diophantiennes suivantes ont des solutions :

1. $5x + 17y = 1$
2. $6x - 8y = 5$
3. $3x - 4y = 10$
4. $21x - 56y = 14$

EXERCICE 5.18.
Résoudre (dans $\mathbb{Z}$) les équations diophantiennes suivantes :

1. $7x + 12y = 1$
2. $12x - 14y = 1$
3. $8x + 12y = 2$
4. $9x - 12y = 3$

EXERCICE 5.19.
Après en avoir justifié l'existence, trouver pour chacune des équations suivantes deux entiers x et y solutions, à l'aide de l'algorithme d'EUCLIDE :

1. $3^7x - 7^3y = 1$
2. $5^{10}x - 2^{10}y = 1$

EXERCICE 5.20.
Existe-t-il un entier n tel que $\frac{n-6}{15}$ et $\frac{n-5}{12}$ soient tous deux entiers ?

EXERCICE 5.21.
Résoudre les équations diophantiennes suivantes :

1. $3x + 4y = 1$
2. $5x - 7y = 4$
3. $5x - 8y = 2$

EXERCICE 5.22.
Déterminer les entiers x et y tels que $6x + 11y = 1$

EXERCICE 5.23.
Résoudre dans $\mathbb{Z}^2$ l'équation $7u + 17v = 3$.