Chapitre 6 – PGCD, théorèmes de Bézout et de Gauss

1. Plus grand diviseur commun

1a. Définition

Soient a et b deux entiers relatifs non tous nuls.
L'ensemble des nombres qui divisent à la fois a et b admet un plus grand élément d, appelé plus grand diviseur commun.
On le note $PGCD(a, b)$, $pgcd(a, b)$ ou bien $a \wedge b$.

Remarque : il existe aussi le plus petit multiple commun de deux nombres, noté $PPCM(a; b)$ ou $a \vee b$.

Exemple 1 Après avoir dressé les listes des diviseurs positifs, calculer les $PGCD$ suivants.
a. $PGCD(30,18)$ **b.** $PGCD(150, -240)$ **c.** $PGCD(84,112)$

Propriétés Pour a et b entiers relatifs, k entier naturel non nul :
- $PGCD(a; b) = PGCD(b; a)$
- $PGCD(a; b) = PGCD(|a|; |b|)$ le signe de a et de b n'a pas d'influence sur le $PGCD$
- $PGCD(a; 0) = |a|$ 0 est multiple de a, car il est multiple de tout entier.
- Si b divise a (on note $b|a$), alors $PGCD(a; b) = b$.
- $\boldsymbol{PGCD(ka; kb) = k \times PGCD(a; b)}$

Exemple 2 On donne $PGCD(296; 555) = 37$. Calculer $PGCD(-296; 555)$ et $PGCD(1110; 592)$.

Exemple 1
a. Les diviseurs de 30 sont $\{1; 2; 3; 5; \mathbf{6}; 10; 15; 30\}$
et les diviseurs de 18 sont $\{1; 2; 3; \mathbf{6}; 9; 18\}$.
Donc $PGCD(30; 18) = \mathbf{6}$.
b. Les diviseurs de 150 sont $\{1; 2; 3; 5; 6; 10; 15; 25; \mathbf{30}; 50; 75; 150\}$
et les diviseurs (positifs) de –240 sont
$\{1; 2; 3; 4; 6; 8; 10; 12; 15; 16; 20; 24; \mathbf{30}; 40; 60; 80; 120; 240\}$
Donc $PGCD(150; -240) = \mathbf{30}$.
c. Les diviseurs de 84 sont $\{1; 2; 3; 4; 6; 7; 12; 14; 21; \mathbf{28}; 42; 84\}$
et les diviseurs de 112 sont $\{1; 2; 4; 7; 8; 14; 16; \mathbf{28}; 56; 112\}$.
Donc $PGCD(84; 112) = \mathbf{28}$.

Exemple 2
$PGCD(-296; 555) = PGCD(296; 555) = \mathbf{37}$
et $PGCD(1\,110; 592) = PGCD(2 \times 555; 2 \times 296) = 2 \times PGCD(555; 296) = \mathbf{74}$.

1b. Nombres premiers entre eux

Si $PGCD(a, b) = 1$, on dit que a et b sont premiers entre eux. Cela veut dire que a et b n'ont pas d'autre diviseur positif commun que 1.

Remarques :

- Une fraction est **irréductible** si et seulement si son numérateur et son dénominateur sont premiers entre eux.
- Soient deux entiers a et b tels que $\boldsymbol{PGCD(a; b) = k}$.

Dans ce cas, on sait qu'on peut « **diviser $\boldsymbol{a}$ et $\boldsymbol{b}$ par $\boldsymbol{k}$** », autrement dit trouver deux entiers a' et b' tels que $a = ka'$ et $b = kb'$. On a alors de plus $PGCD(a'; b') = 1$, donc a' et b' premiers entre eux.

Exemple 1

Déterminer tous les entiers naturels n tels que $PGCD(n, 324) = 12$.

En déduire, parmi ces entiers, tous ceux qui sont inférieurs à 100.

Exemple 2 Déterminer tous les entiers naturels a et b, avec $a < b$, tels que

a. $ab = 432$ et $PGCD(a, b) = 6$ **b.** $a + b = 24$ et $PGCD(a, b) = 4$.

Exemple 1 Si $PGCD(n\,; 324) = 12$, cela signifie que n est divisible par 12.
Il existe alors n' tel que $\boldsymbol{n = 12n'}$. On a alors :
$PGCD(n; 324) = 12$
$\Leftrightarrow PGCD(12n'; 12 \times 27) = 12$
$\Leftrightarrow 12 \times PGCD(n'; 27) = 12$
$\Leftrightarrow \boldsymbol{PGCD(n'; 27) = 1}$
Or $27 = 3 \times 3 \times 3$, donc les entiers n' premiers avec 27 sont les nombres **non multiples de 3**, de la forme $3k + 1$ ou $3k + 2$.
Ainsi, les entiers $n = 12n'$ qui conviennent sont tous les nombres de la forme $\boldsymbol{12(3k + 1)}$ ou $\boldsymbol{12(3k + 2)}$ avec $k \in \mathbb{N}$.
Ceux qui sont inférieurs à 100 sont : $\{\boldsymbol{12; 24; 48; 60; 84; 96}\}$.

Exemple 2 **a.** Comme $PGCD(a; b) = 6$, a et b sont multiples de 6.
Il existe alors a' et b' entiers tels que $\boldsymbol{a = 6a'}$ et $\boldsymbol{b = 6b'}$.
Ainsi, $PGCD(a; b) = 6 \Leftrightarrow PGCD(6a'; 6b') = 6 \Leftrightarrow \boldsymbol{PGCD(a'; b') = 1}$.
De plus, $ab = 432 \Leftrightarrow 6a' \times 6b' = 432 \Leftrightarrow a' \times 6b' = 72 \Leftrightarrow \boldsymbol{a'b' = 12}$.
Les seuls couples de nombres $(a'; b')$ dont le produit est 12, qui sont premiers entre eux et tels que $a' < b'$ sont $\boldsymbol{(1; 12)}$ **et** $\boldsymbol{(3; 4)}$.
Or $a = 6a'$ et $b = 6b'$, donc les couples $(a; b)$ solution sont $\boldsymbol{(6; 72)}$ **et** $\boldsymbol{(18; 24)}$.
b. Comme $PGCD(a; b) = 4$, a et b sont multiples de 4.
Il existe alors a' et b' entiers tels que $\boldsymbol{a = 4a'}$ et $\boldsymbol{b = 4b'}$.
Ainsi, $PGCD(a; b) = 4 \Leftrightarrow PGCD(4a'; 4b') = 4 \Leftrightarrow \boldsymbol{PGCD(a'; b') = 1}$.
De plus, $a + b = 24 \Leftrightarrow 4a' + 4b' = 24 \Leftrightarrow 4(a' + b') = 4 \times 6 \Leftrightarrow \boldsymbol{a' + b' = 6}$.
Le seul couple de nombres $(a'; b')$ dont la somme est 6, qui sont premiers entre eux et tels que $a' < b'$ est $\boldsymbol{(1; 5)}$.
Or $a = 4a'$ et $b = 4b'$, donc le couple $(a; b)$ solution est $\boldsymbol{(4; 20)}$.

2. Algorithme d'Euclide

2a. PGCD et reste

Propriété : Soient a et b entiers. Soit r le reste dans la division euclidienne de a par b. Alors $PGCD(a,b) = PGCD(b,r)$.

Démonstration :
Soit $d = PGCD(a,b)$ et $d' = PGCD(b,r)$. Il faut montrer que $d = d'$.
On pose $a = bq + r$ la division euclidienne de a par b.
• d divise a et b, et $r = a - bq$ est une combinaison linéaire de a et b.
Ainsi, d divise r (et b) : on a $d \leq d'$.
• d' divise b et r, et $a = bq + r$ est une combinaison linéaire de b et r.
Ainsi, d' divise a (et b) : on a $d' \leq d$.
• Comme $d \leq d'$ et $d' \leq d$, on en déduit que $d = d'$.

2b. Algorithme d'Euclide

Pour trouver $PGCD(a, b)$, on détermine les restes successifs de la division euclidienne de a par b, puis de b par r… et ainsi de suite jusqu'à obtenir un reste nul.
Le $PGCD$ de a et b est alors le dernier reste non nul obtenu.

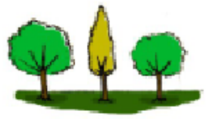
Remarque : Il existe un algorithme « par soustractions successives » plus lent , parfois étudié au collège, qui se base sur le fait que $\boldsymbol{PGCD(a,b) = PGCD(b, a-b)}$.

Exemple 1 Calculer $PGCD(144; 820)$ et $PGCD(202; 138)$ à l'aide de l'algorithme d'Euclide, en détaillant les divisions euclidiennes effectuées.

Exercice 2 A l'aide de l'algorithme d'Euclide, dire si les nombres 4 847 et 5 633 sont premiers entre eux.

Exercice 3 Donner le code d'une fonction Python `pgcd(a,b)` qui calcule le $PGCD$ de a et b avec $a > b$.

Exercice 4 A l'aide de l'algorithme d'Euclide, déterminer $PGCD(a, b)$ avec $a = 18\,440$ et $b = 9\,828$.
La fraction $\frac{a}{b}$ est-elle irréductible ?



Exercice 5 Un terrain rectangulaire a pour dimensions 966 m et 1 008 m.
Sur ses côtés, on veut planter des arbres régulièrement espacés d'un nombre entier de mètres.
Il doit y avoir un arbre à chaque côté du terrain. Quel est le nombre minimum d'arbres que l'on pourra planter ?

Exemple 1

• $PGCD(144; 820)$	$820 = 144 \times 5 + \mathbf{100}$
$= PGCD(144; 100)$	$144 = 100 \times 1 + \mathbf{44}$
$= PGCD(100; 44)$	$100 = 44 \times 2 + \mathbf{12}$
$= PGCD(44; 12)$	$44 = 12 \times 3 + \mathbf{8}$
$= PGCD(12; 8)$	$12 = 8 \times 1 + \mathbf{4}$
$= PGCD(8; 4)$	$8 = 4 \times 2 + \mathbf{0}$
$= PGCD(4; 0) = \mathbf{4}$	

• $PGCD(202; 138)$	$202 = 138 \times 1 + \mathbf{64}$
$= PGCD(138; 64)$	$138 = 64 \times 2 + \mathbf{10}$
$= PGCD(64; 10)$	$64 = 10 \times 6 + \mathbf{4}$
$= PGCD(10; 4)$	$10 = 4 \times 2 + \mathbf{2}$
$= PGCD(4; 2)$	$4 = 2 \times 2 + \mathbf{0}$
$= PGCD(2; 0) = \mathbf{2}$	

Exemple 2

$PGCD(5633; 4847)$	$5633 = 4847 \times 1 + \mathbf{786}$
$= PGCD(4847; 786)$	$4847 = 786 \times 6 + \mathbf{131}$
$= PGCD(786; 131)$	$786 = 131 \times 6 + \mathbf{0}$
$= PGCD(131; 0) = \mathbf{131}$	

Donc 5 633 et 4 847 ne sont **pas premiers entre eux**, car ils sont multiples de 131.

Exemple 3

```
def pgcd(a,b) :
  while b > 0 :
    r = a % b
    a = b
    b = r

  return a
```

Exemple 4

$PGCD(18440; 9828)$ $\quad$ $18440 = 9828 \times 1 + \mathbf{8612}$
$= PGCD(9828; 8612)$ $\quad$ $9828 = 8612 \times 1 + \mathbf{1216}$
$= PGCD(8612; 1216)$ $\quad$ $8612 = 1216 \times 7 + \mathbf{100}$
$= PGCD(1216; 100)$ $\quad$ $1216 = 100 \times 12 + \mathbf{16}$
$= PGCD(16; 12)$ $\quad$ $16 = 12 \times 1 + \mathbf{4}$
$= PGCD(12; 4)$ $\quad$ $12 = 4 \times 3 + \mathbf{0}$
$= PGCD(4; 0) = \mathbf{4}$

Donc la fraction $\frac{18\,440}{9\,828}$ n'est **pas irréductible** : on peut la simplifier par 4.

Exemple 5

Pour planter un minimum d'arbres, l'espacement entre les arbres doit être le plus grand possible : cela correspond au PGCD de la largeur et de la longueur.

$PGCD(1008; 966)$ $\quad$ $1008 = 966 \times 1 + \mathbf{42}$
$= PGCD(966; 42)$ $\quad$ $966 = 42 \times 23 + \mathbf{0}$
$= PGCD(42; 0) = \mathbf{42}$

Ainsi, les arbres seront espacés de 42 m.
Le périmètre total du terrain est $2(1\,008 + 966) = 3\,948$ m.
Or $3\,948 \div 42 = 94$, donc on pourra planter au minimum **94 arbres**.

3. Théorème de Bézout

3a. Identité de Bézout

Soient a et b non nuls. Alors il existe un couple d'entiers $(u; v)$ tels que :

$$au + bv = PGCD(a, b)$$

Corollaire : Tout diviseur commun à a et b divise $PGCD(a, b)$.

Démonstration de l'identité de Bézout :
Soit $\mathcal{E}$ l'ensemble des combinaisons linéaires strictement positives de a et b, c'est-à-dire des nombres de la forme $ax + by$ avec x, y entiers.
$\mathcal{E}$ est un ensemble d'entiers positifs non vide (par exemple, $|a| \in \mathcal{E}$), donc il contient un plus petit élément, que l'on note d.
$d \in \mathcal{E}$, donc il existe deux entiers u et v tels que $d = au + bv$.
Soit $D = PGCD(a, b)$. Montrons que $d = D$, cela prouvera la propriété.
• D divise a et b, donc D divise $au + bv = d$. Ainsi, $D \leq d$.
• Montrons que d divise a.
On effectue la division euclidienne de a par d : $a = dq + r$ avec $0 \leq r < d$.
Alors $r = a - dq = a - (au + bv)q = a(1 - uq) + b(-vq)$
r est donc une combinaison linéaire de a et b.
Si $r > 0$, alors r serait un élément de $\mathcal{E}$, or c'est absurde : par définition, d est le plus petit élément de $\mathcal{E}$ alors que $0 \leq r < d$.
Ainsi, $r = 0$, et d divise a.
On montre de même que d divise b.
Ainsi, d divise a et b, donc $d \leq D$ (D étant leur plus grand diviseur commun).
Conclusion : $d \leq D$ et $D \leq d$, on en déduit que $d = D$.

Démonstration du corollaire : Soit d, un diviseur commun à a et b.
Alors d divise toute combinaison linéaire de a et b.
D'après l'identité de Bézout, le $PGCD$ de a et b est une combinaison linéaire de a et de b. Donc d divise ce $PGCD$.

Exemples
a. Déterminer D, le $PGCD$ de 42 et 15. Puis trouver deux nombres entiers u et v tels que $42u + 15v = D$.
b. Même question avec 180 et 75.

a. En appliquant l'algorithme d'Euclide, on trouve $PGCD(42; 15) = \mathbf{3}$.
Or on peut se rappeler que $3 \times 15 = 45$, donc on a $42 \times (-1) + 15 \times 3 = \mathbf{3}$.
Ainsi, le couple $(u; v)$ est $(\mathbf{-1}; \mathbf{3})$.
b. En appliquant l'algorithme d'Euclide, on trouve $PGCD(180; 75) = \mathbf{15}$.
Ici, c'est un peu plus difficile, mais $2 \times 180 = 360$ et $5 \times 75 = 375$.
Donc $-2 \times 180 + 5 \times 75 = \mathbf{15}$ et le couple $(u; v)$ est égal à $(\mathbf{-2}; \mathbf{5})$.

3b. Théorème de Bézout, algorithme d'Euclide étendu

Les entiers a et b sont premiers entre eux si et seulement si il existe un couple d'entiers (u, v) tels que $au + bv = 1$.

Remarque : Contrairement à l'identité de Bézout qui est une implication, on a ici une équivalence.

Démonstration :
$\Longrightarrow$: si a et b sont premiers entre eux, alors leur $PGCD$ est 1.
D'après l'identité de Bézout, il existe u et v entiers tels que $au + bv = 1$.
$\Longleftarrow$: s'il existe u et v entiers tels que $au + bv = 1$, soit d un diviseur commun à a et b.
Alors d divise $au + bv$, c'est à dire 1. Le seul diviseur de 1 est 1, donc $d = 1$. On en en déduit que le plus grand diviseur commun à a et b est 1.

La démonstration prouve qu'il existe des entiers u et v tels que $\boldsymbol{au + bv = 1}$, mais n'explique pas comment les trouver. Pour cela, on utilise **l'algorithme d'Euclide étendu** : tout en appliquant l'algorithme d'Euclide, on réécrit les divisions euclidiennes sous la forme $\boldsymbol{r = a - bq}$, et on **injecte le reste dans la division euclidienne suivante**. On pourra donc toujours exprimer **chaque reste successif en fonction de $\boldsymbol{a}$ et de $\boldsymbol{b}$**.

Exemple 1 Trouver le couple de Bézout de 47 et 25.

Cette méthode fonctionne aussi quand les nombres ne sont pas premiers entre eux.
Exemple 2 Trouver le couple de Bézout de 243 et 198.

Contrairement à l'identité de Bézout, le théorème est une équivalence : si on parvient à **obtenir une égalité $\boldsymbol{au + bv = 1}$**, cela implique que a et b sont **premiers entre eux**.
Exemple 3 Démontrer que 33 et 65 sont premiers entre eux sans utiliser les diviseurs ou le $PGCD$.
Exemple 4 Démontrer que pour tout entier n, les entiers $(2n + 1)$ et $(3n + 2)$ sont premiers entre eux.

Exemple 1

$47 = 25 \times 1 + 22$ $\qquad$ $\begin{aligned} \mathbf{22} &= 47 - 25 \times 1 \\ &= 1 \times 47 - 1 \times 25 \end{aligned}$

$25 = 22 \times 1 + 3$ $\qquad$ $\begin{aligned} \mathbf{3} &= 25 - \mathbf{22} \times 1 \\ &= 25 - (1 \times 47 - 1 \times 25) \times 1 \\ &= -1 \times 47 + 25 \times 2 \end{aligned}$

$22 = 3 \times 7 + 1$ $\qquad$ $\begin{aligned} \mathbf{1} &= \mathbf{22} - \mathbf{3} \times 7 \\ &= (1 \times 47 - 1 \times 25) - (-1 \times 47 + 25 \times 2) \times 7 \\ &= 8 \times 47 - 15 \times 25 \end{aligned}$

Ainsi, on a $47u + 25v = 1$ avec $u = 8$ et $v = -15$.

Exemple 2

$243 = 198 \times 1 + 45$ $\quad$ $\mathbf{45} = 243 - 198 \times 1$
$= 1 \times 243 - 1 \times 198$

$198 = 45 \times 4 + 18$ $\quad$ $\mathbf{18} = 198 - \mathbf{45} \times 4$
$= 198 - (1 \times 243 - 1 \times 198\ ) \times 4$
$= -4 \times 243 + 5 \times 198$

$45 = 18 \times 2 + 9$ $\quad$ $\mathbf{9} = \mathbf{45} - \mathbf{18} \times 2$
$= (1 \times 243 - 1 \times 198) - (-4 \times 243 + 5 \times 198) \times 2$
$= 9 \times 243 - 11 \times 198$

$18 = 9 \times 2 + 0$
On trouve un reste nul, donc $PGCD(243{,}198) = 9$
et on a $243u + 198v = 9$ avec $u = 9$ et $v = -11$.

Exemple 3
$33 \times 2 = 66$, donc $33 \times 2 - 65 \times 1 = 1$.
Ainsi, $(\mathbf{2}; -\mathbf{1})$ **est un couple de Bézout** $(u; v)$ tel que $33u + 65v = \mathbf{1}$, donc d'après le théorème de Bézout, 33 et 65 sont **premiers entre eux**.

Exemple 4
Cherchons u et v tels que $u(2n + 1) + v(3n + 2) = 1$.
Pour supprimer les termes en n, on peut prendre $u = -3$ et $v = 2$.
On a alors $-3(2n + 1) + 2(3n + 2) = -6n - 3 + 6n + 4 = \mathbf{1}$.
Ainsi, il existe un couple de Bézout $(u; v)$ tels que $u(2n + 1) + v(3n + 2) = 1$.
Donc pour tout entier $n \in \mathbb{Z}$, **les nombres** $(\mathbf{2n + 1})$ **et** $(\mathbf{3n + 2})$ **sont premiers entre eux**.

4. Théorème de Gauss

4a. Énoncé

Soient a, b et c trois entiers non nuls.
Si a divise le produit bc et si a et b sont premiers entre eux, alors a divise c.

Autrement dit : ($a|bc$ et $PGCD(a,b) = 1$) $\Longrightarrow a|c$

Démonstration : $a|bc$, donc il existe k entier tel que $bc = ka$.
D'après Bézout, il existe aussi u et v entiers tels que :

$$au + bv = 1$$

On multiplie par c :

$$acu + bcv = c$$
$$\Leftrightarrow acu + kav = c$$
$$\Leftrightarrow a(cu + kv) = c$$

donc $a|c$.

Le théorème de Gauss s'applique quand un nombre divise un produit alors qu'il est premier avec un des facteurs.

Exemple 1

a. Trouver tous les couples d'entiers relatifs $(x; y)$ tels que $5(x-1) = 7y$.

b. En déduire les couples d'entiers relatifs $(x; y)$ tels que $5x + 7y = 5$.

Exemple 2

a. Déterminer les couples d'entiers relatifs $(x; y)$ tels que $7(x-3) = 5(y-2)$.

b. En déduire les entiers relatifs x tels que $7x \equiv 1[5]$.

Exemple 1

a. 5 divise le produit $7y$ et 5 et 7 sont premiers entre deux, donc d'après le théorème de Gauss, 5 divise y.
Il existe alors k tel que $y = 5k$. Ainsi :
$5(x-1) = 7y \Leftrightarrow 5(x-1) = 5 \times 7k \Leftrightarrow x - 1 = 7k \Leftrightarrow x = 7k + 1$.
Ainsi, les couples qui conviennent sont ceux de la forme $(\boldsymbol{7k+1}; \boldsymbol{5k})$ avec $k \in \mathbb{Z}$.
Ce sont par exemple $(1; 0); (8; 5); (15; 10)$ ...
On vérifie bien que pour tout k, ces couples vérifient l'égalité.

b. $5(x-1) = 7y \Leftrightarrow 5x - 5 = 7y \Leftrightarrow 5x - 7y = 5$.
Ainsi, pour tout couple $(x; y)$ vérifiant l'égalité de la question **a**, le couple $(x; -y)$ vérifie l'égalité de la question **b.**
Ainsi, les couples correspondants sont ceux de la forme $(\boldsymbol{7k+1}; \boldsymbol{-5k})$ avec $k \in \mathbb{Z}$.

Exemple 2

a. 7 divise le produit $5(y-2)$ et 7 et 5 sont premiers entre eux, donc d'après le théorème de Gauss, 7 divise $(y-2)$.
Il existe alors k entier tel que $y-2=7k \Leftrightarrow y=7k+2$.
On a alors $7(x-3)=5(7k+2-2) \Leftrightarrow 7x-21=35k \Leftrightarrow 7x=35k+21 \Leftrightarrow x=5k+3$.
Ainsi, les couples solution sont de la forme $(\mathbf{5}\boldsymbol{k}+\mathbf{3}; \mathbf{7}\boldsymbol{k}+\mathbf{2})$ avec $k \in \mathbb{N}$.
Ce sont par exemple $(3;2)$; $(8;9)$; $(13;16)$…
On vérifie bien que pour tout k, ces couples vérifient l'égalité.
b. $7(x-3)=5(y-2) \Leftrightarrow 7x-21=5y-10 \Leftrightarrow 7x=5y+11 \Longrightarrow 7x \equiv 1[5]$.
Réciproquement, si $7x \equiv 1[5]$, alors $7x \equiv 11[5]$ et $7x=5k+11$ avec $k \in \mathbb{Z}$.
Ainsi, on en déduit avec la question **a** que $7x \equiv 1[5]$ si et seulement si $\boldsymbol{x}$ **est de la forme** $\mathbf{5}\boldsymbol{k}+\mathbf{3}$ avec $k \in \mathbb{Z}$.

4b. Diviseurs premiers entre eux

Corollaire : Soient a, b et c trois entiers non nuls.
Si b et c divisent a, et si b et c sont premiers entre eux, alors bc divise a.

Autrement dit : $(\ b|a \ \text{ et } \ c|a \ \text{ et } \ PGCD(b,c) = 1\ ) \Longrightarrow bc|a$

Démonstration : $b|a$ et $c|a$, donc il existe k et k' entiers tels que $a = kb$ et $a = k'c$.
Ainsi, $kb = k'c$ donc b divise $k'c$. Or b et c sont premiers entre eux, donc d'après le théorème de Gauss, b divise k'.
Ainsi, il existe k'' tel que $k' = k''b$.
Or $a = k'c = k''bc$ et ainsi bc divise a.

Remarque Il est nécessaire que b et c soient premiers entre eux.
Ainsi, $6|12$ et $4|12$, mais 6 et 4 ne sont pas premiers entre eux. D'ailleurs, $6 \times 4 = 24$ et on n'a pas $24|12$…
En revanche, $3|75$ et $5|75$, et 3 et 5 sont premiers entre eux, donc $15|75$.

Exemple Soit n un entier naturel. Montrer que $n(n+1)(n+2)$ est divisible par 6.

Parmi n, $(n+1)$ et $(n+2)$, il existe nécessairement un multiple de 2, et un multiple de 3.
Donc 2 et 3 divisent $n(n+1)(n+2)$. Or 2 et 3 sont premiers.
D'après le corollaire du théorème de Gauss, $3 \times 2 =$ **6 divise** $\boldsymbol{n(n+1)(n+2)}$.

4c. Équations diophantiennes linéaires

Propriété : L'équation diophantienne $ax + by = c$, d'inconnues x et y, admet des solutions si et seulement si c est un multiple de $PGCD(a, b)$.

Démonstration : Soit $D = PGCD(a, b)$.

$\Longrightarrow$: supposons que l'équation $ax + by = c$ ait un couple solution (x, y).

• D'après le théorème de Bézout, il existe u et v entiers tels que :

$$au + bv = D$$

• D'autre part, on effectue la division euclidienne de c par D : $c = Dq + r$ avec $r < D$. Ainsi,

$$ax + by = Dq + r$$

En additionnant les deux égalités obtenues :

$$a(u + x) + b(v + y) = D(q + 1) + r$$
$$\Leftrightarrow r = a(u + x) + b(v + y) - D(q + 1)$$

Or a, b et D sont des multiples de D.
r est donc un multiple de D, mais $r < D$ par définition.
Donc $r = 0$ et c est bien un multiple de D.

$\Longleftarrow$: si c est un multiple de D,
alors il existe k entier tel que $c = kD$.
D'après l'identité de Bézout, il existe u et v entiers tels que

$$au + bv = D$$

En multipliant cette égalité par k, on trouve :

$$aku + bkv = kD = c$$

Donc l'équation $ax + by = c$ a pour solution le couple (ku, kv).

Si on dispose d'une solution particulière, **le théorème de Gauss permet d'en déduire toutes les autres**.

Exemple 1 Soit l'équation (E) à valeurs dans $\mathbb{Z}$: $17x - 33y = 1$.

a. Démontrer que cette équation admet des solutions.

b. Déterminer une solution particulière de l'équation (E).

c. Soit une autre solution $(x; y)$. A l'aide de la question **b**, établir une égalité permettant d'appliquer le théorème de Gauss. En déduire toutes les solutions de (E). Vérifier que les solutions trouvées conviennent.

Exemple 2 Déterminer toutes les solutions de l'équation (E): $29x + 13y = 6$

Exemple 1

a. 17 et 33 sont premiers entre eux, donc **d'après l'identité de Bézout**, il existe bien un couple d'entiers $(x; y)$ tel que $17x - 33y = 1$.

b. On pourrait appliquer l'algorithme d'Euclide étendu, mais on trouve assez facilement le couple $(\mathbf{2}; \mathbf{1})$.

c. On sait alors que $17x - 33y = 1$, mais aussi que $17 \times 2 - 33 \times 1 = 1$.
On en déduit que $17x - 33y = 17 \times 2 - 33 \times 1 \Leftrightarrow 17(x - 2) = 33(y - 1)$.

Ainsi, 17 divise le produit $33(y-1)$ mais 17 et 33 sont premiers entre eux, donc 17 divise $(y-1)$. Ainsi, $y-1=17k \Leftrightarrow y=17k+1$.
Ainsi, $17(x-2)=33(17k+1-1) \Leftrightarrow 17x-34=33\times 17k \Leftrightarrow x=33k+2$.
Les solutions sont donc les couples de la forme $(\boldsymbol{33k+2}; \boldsymbol{17k+1})$.
On vérifie bien que $17x-33y=17(33k+2)-33(17k+1)=34-33=1$.

Exemple 2
29 et 13 sont premiers entre eux, donc il existe même des nombres x' et y' tels que $29x'+13y'=1$. L'algorithme d'Euclide étendu nous donne $x'=-4$ et $y'=9$.
Ainsi, un couple solution de l'équation $29x+13y=6$ est donc $(6x' ; 6y')$, soit $(\boldsymbol{-24} ; \boldsymbol{54})$.
Soit $(x ; y)$ un autre couple solution.
On sait alors que $29x+13y=29\times(-24)+13\times 54$
Donc $29(x+24)=13(54-y)$.
D'après le théorème de Gauss, 29 divise le produit $13(54-y)$, donc 29 divise $(54-y)$. Ainsi, $54-y=29k \Leftrightarrow y=54-29k$ avec $k\in\mathbb{Z}$. Par conséquent :
$29(x+24)=13(54-54+29k)$
$\Leftrightarrow 29x+29\times 24=13\times 29k$
$\Leftrightarrow x+24=13k$
$\Leftrightarrow x=13k-24$.
Donc les couples solution sont de la forme $(\boldsymbol{13k-24}; \boldsymbol{54-29k})$ avec $k\in\mathbb{Z}$.