CHAPITRE 3 : PGCD, Euclide, Bézout, Gauss.

CHAPITRE 3 : PGCD, Euclide, Bézout, Gauss.

1 PGCD

1.1 Définition du PGCD

Soit a et b deux entiers relatifs *non nuls simultanément*.

L'ensemble des diviseurs communs à a et b admet un plus grand élément appelé le PGCD[1] de a et b

Exemples :

- Quel est le $PGCD(6\,,10)$?

L'ensemble des diviseurs de 6 est $D(6) = \{-6\,;-3\,;-2\,;-1\,;\ 1\,;\ 2\,;\ 3\,;\ 6\}$
L'ensemble des diviseurs de 10 est $D(10) = \{-10\,;-5\,;-2\,;-1\,;\ 1\,;\ 2\,;\ 5\,;\ 10\}$
L'ensemble des diviseurs communs à 6 et 10 est $D(6) \cap D(10) = \{-2\,;-1\,;\ 1\,;\ \mathbf{2}\}$

$$PGCD(6\,,10) = \mathbf{2}$$

- Soit $a \in \mathbb{N}^*$. Quel est le $PGCD(a\,,0)$?

L'ensemble des diviseurs de a est $D(a) = \{-a\,;\ldots\,;\ldots\,;-1\,;\ 1\,;\ldots\,;\ldots\,;\ a\}$
L'ensemble des diviseurs de 0 est $D(0) = \mathbb{Z}^*$.
L'ensemble des diviseurs communs à a et 0 est $D(a) \cap D(0) = \{-a\,;\ldots\,;\ldots\,;-1\,;\ 1\,;\ldots\,;\ldots\,;\ \boldsymbol{a}\}$

$$PGCD(a\,,0) = \boldsymbol{a}$$

- Soit $a \in \mathbb{N}^*$. Quel est le $PGCD(a\,,1)$?

L'ensemble des diviseurs de a est $D(a) = \{-a\,;\ldots\,;\ldots\,;-1\,;\ 1\,;\ldots\,;\ldots\,;\ a\}$
L'ensemble des diviseurs de 1 est $D(1) = \{-1\,;1\}$.
L'ensemble des diviseurs communs à a et 1 est $D(a) \cap D(1) = \{-1\,;\mathbf{1}\}$

$$PGCD(a\,,1) = \mathbf{1}$$

- Soit $a \in \mathbb{N}^*$. Quel est le $PGCD(a\,,a)$?

L'ensemble des diviseurs de a est $D(a) = \{-a\,;\ldots\,;\ldots\,;-1\,;\ 1\,;\ldots\,;\ldots\,;\ a\}$
L'ensemble des diviseurs communs à a et a est $D(a) \cap D(a) = \{-a\,;\ldots\,;\ldots\,;-1\,;\ 1\,;\ldots\,;\ldots\,;\ \boldsymbol{a}\}$

$$PGCD(a\,,a) = \boldsymbol{a}$$

Détermination à la calculatrice :

Ces fonctions sont présentes sur les calculatrices TI82 et TI83 (touche Math NUM)
Pour le PGCD : Math NUM 9
Les arguments négatifs ne sont pas acceptés. Dans ce cas, les remplacer par leurs opposés positifs étant donné que $PGCD(a\,,b) = PGCD(\pm a\,,\pm\, b)$

[1] **PGCD :** Plus Grand Commun Diviseur

1.2 Détermination à l'aide de la décomposition en facteurs premiers

Si a et b sont deux entiers supérieurs ou égaux à 2 :
Le $PGCD(a\,,b)$ est égal au produit des facteurs premiers communs aux deux nombres, chacun étant affecté **du plus petit exposant** avec lequel il figure dans leurs décompositions :

Exemple :

Recherche du $PGCD(234\,;\,84)$ par la méthode des facteurs premiers :

234	2
117	3
39	3
13	13
1	

$234 = 2^1 \times 3^2 \times 13$

84	2
42	2
21	3
7	7
1	

$84 = 2^2 \times 3^1 \times 7$

$$PGCD(234\,;\,84) = 2^1 \times 3^1 = \mathbf{6}$$

Démonstration du calcul du PGCD à partir des facteurs premiers :

Soit les décompositions en facteurs premiers de a et b :

$$a = {p_1}^{\alpha_1} \times {p_2}^{\alpha_2} \times \ldots \times {p_n}^{\alpha_n}$$
$$b = {p_1}^{\beta_1} \times {p_2}^{\beta_2} \times \ldots \times {p_n}^{\beta_n}$$

où $p_1, p_2, \ldots, p_n$, sont les **premiers nombres premiers** et où $\alpha_1, \alpha_2, \ldots, \alpha_n, \beta_1, \beta_2, \ldots, \beta_n$ sont des entiers naturels éventuellement nuls.

Tout entier d diviseur commun à a et b a une décomposition de la forme ${p_1}^{\gamma_1} \times {p_2}^{\gamma_2} \times \ldots \times {p_n}^{\gamma_n}$ avec γ_i vérifiant :

$0 \leq \gamma_i \leq \alpha_i$ car d divise a et $0 \leq \gamma_i \leq \beta_i$ car d divise b

Si δ_i désigne le plus petit des entiers (α_i, β_i) alors $0 \leq \gamma_i \leq \delta_i$

Le PGCD est obtenu lorsque $\gamma_1 = \delta_1, \gamma_2 = \delta_2$, ..., $\gamma_n = \delta_n$

Exemple :

$$234 = 2^1 \times 3^2 \times 7^0 \times 13^1 \; et \; 84 = 2^2 \times 3^1 \times 7^1 \times 13^0$$

D'où :

$$PGCD(234\,;\,84) = 2^1 \times 3^1 \times 7^0 \times 13^0 = \mathbf{6}$$

1.3 Relation entre la divisibilité de a par b et le PGCD(a ; b)

Soit a et b deux entiers naturels. Si $b|a$ alors $PGCD(a\,;\,b) = b$

Démonstration :

Soit $d \in \mathbb{N}$.
Si $d|b$, comme $b|a$, alors $d|a$. Tout diviseur d de b est aussi un diviseur de a. Le plus grand diviseur de b étant b lui-même, alors le plus grand diviseur commun à a et b est $PGCD(a\,;\,b) = b$

1.4 Propriété fondamentale des diviseurs communs :

Soit $a \in \mathbb{Z}^*$ et $b \in \mathbb{Z}$. Si $\boldsymbol{a = bk + r}$ où $k \in \mathbb{Z}$ et $r \in \mathbb{Z}$, alors :

Les diviseurs communs à $\boldsymbol{a}$ *et* $\boldsymbol{b}$ ***sont les mêmes*** *que les diviseurs communs* à $\boldsymbol{b}$ *et* $\boldsymbol{r}$**.**

Ce qui s'écrit : $D(a) \cap D(b) = D(b) \cap D(r)$

Conséquence :

$$PGCD(a\,;b) = PGCD(b\,;r)$$

Remarque :

On n'a pas la condition $0 \leq r < b$ donc $\boldsymbol{a = bk + r}$ n'est pas obligatoirement la relation de la division euclidienne de *a* par *b* er $\boldsymbol{r}$ n'est pas obligatoirement le reste.

Exemple :

Soit $a = 20$ et $b = 6$.

Soit E l'ensemble des diviseurs communs à a et b.

$E = D(20) \cap D(6)$

$E = \{-20\,;-10\,;-5\,;-4\,;-2\,;-1\,;\,1\,;\,2\,;\,4\,;\,10\,;\,20\} \cap \{-6\,;-3\,;-2\,;-1\,;\,1\,;\,2\,;\,3\,;\,6\}$

$E = \{-2\,;-1\,;\,1\,;\,2\}$

et $PGCD(20\,;6) = 2$

Si on écrit a sous la forme $a = bk + r$, on aura par exemple : $\mathbf{20 = 6 \times 2 + 8}$

Donc ici, $k = 2$ et $r = 8$

D'après la propriété fondamentale des diviseurs communs, on a :

« L'ensemble des diviseurs communs à a et b et l'ensemble des diviseurs communs à b et r **sont identiques ».**

Illustration sur un exemple :

Soit F l'ensemble des diviseurs communs à b et r.

$F = D(6) \cap D(8)$

$F = \{-6\,;-3\,;-2\,;-1\,;\,1\,;\,2\,;\,3\,;\,6\} \cap \{-8\,;-4\,;-2\,;-1\,;\,1\,;\,2\,;\,4\,;\,8\}$

$F = \{-2\,;-1\,;\,1\,;\,2\}$

et $PGCD(6\,;8) = 2$

Démonstration :

Soit $a \in \mathbb{Z}^*$ et $b \in \mathbb{Z}$. Si $\boldsymbol{a = bk + r}$ où $k \in \mathbb{Z}$ et $r \in \mathbb{Z}$

Soit E l'ensemble des diviseurs communs à a et b. $E = D(a) \cap D(b)$

Soit F l'ensemble des diviseurs communs à b et r. $F = D(b) \cap D(r)$

Pour montrer que $E = F$, on montre que si $d \in E$ alors $d \in F$ puis on montre que si $d \in F$ alors $d \in E$.

- Si $\boldsymbol{d \in E}$

$\boldsymbol{d \in E}$, alors d divise b et donc d divise bk.

$\boldsymbol{d \in E}$, alors d divise a.

Donc d divise toute combinaison linéaire de a et bk, donc en particulier, d divise $a - bk = r$.
Comme d est un diviseur à la fois de b et de r, alors $\boldsymbol{d \in F}$

- si $\boldsymbol{d \in F}$

$\boldsymbol{d \in F}$, alors d divise b et donc d divise bk.

$\boldsymbol{d \in F}$, alors d divise r.

Donc d divise toute combinaison linéaire de r et bk, donc en particulier, d divise $a = bk + r$.
Comme d est un diviseur à la fois de b et de a, alors $\boldsymbol{d \in E}$

Conclusion :
L'ensemble des diviseurs **de $\boldsymbol{a}$ et $\boldsymbol{b}$** et l'ensemble des diviseurs **de $\boldsymbol{b}$ et $\boldsymbol{r}$** sont identiques, lorsqu'on a $\boldsymbol{a = bk + r}$. Cela est vrai même si ce n'est pas une relation de division euclidienne.

Comme les ensembles de diviseurs sont identiques, les PGCD aussi sont identiques : $PGCD(a\,;b) = PGCD(b\,;r)$.

Remarques :

Puisque $r = a - bk$ on peut écrire :
Pour tout $k \in \mathbb{Z}$: $D(a) \cap D(b) = D(b) \cap D(r) = D(b) \cap D(a - bk)$
En prenant $k = -1$ on a : $D(a) \cap D(b) = D(b) \cap D(a + b)$
En prenant $k = 1$ on a : $D(a) \cap D(b) = D(b) \cap D(a - b)$
etc.
Par exemple avec $k = 5$,

$$D(234) \cap D(84) = D(84) \cap D(234 - 84 \times 5)$$
$$D(234) \cap D(84) = D(84) \cap D(-186)$$

Conséquence de la propriété fondamentale des diviseurs communs :

Le PGCD de deux nombres $a \in \mathbb{Z}^*$ et $b \in \mathbb{Z}$ reste inchangé si on remplace l'un des deux nombres par exemple a par la différence $a - kb$ avec $k \in \mathbb{Z}$.

$$PGCD(a\,;\,b) = PGCD(b\,;\,a - kb).$$

2 L'algorithme d'Euclide

2.1 Théorème de l'algorithme d'Euclide

a et b sont deux entiers naturels *non nuls* tels que $0 < b \leq a$.
Soit la suite des divisions euclidiennes :

- Division de a par b : $a = bq_0 + r_0$
- Division de b par r_0 : $b = r_0q_1 + r_1$
- Division de r_0 par r_1 : $r_0 = r_1q_2 + r_2$
- …..
- Division de r_{n-1} par r_n : $r_{n-1} = r_nq_{n+1} + r_{n+1}$

Cette suite de divisions finit par s'arrêter lorsqu'un des restes r_i est nul.
Le ***dernier reste non nul*** **est le $PGCD(a\,,b)$.**
Au cas où, dès la première division, le reste r_0 est nul alors $b|a$ et $PGCD(a\,,b) = b$.

Remarque : Ce résultat permet de calculer le $PGCD(a\,,b)$ sous forme algorithmique. Ce processus itératif[2] où, à chaque étape le dividende a est remplacé par le diviseur b et le diviseur b est remplacé par le reste r est appelé Algorithme d'Euclide.

Exemple :
Calculer **en utilisant l'algorithme d'Euclide** : $PGCD(234\,;\,84)$.

Réponse :
On écrit les relations des divisions euclidiennes successives $a = bq + r\ avec\ 0 \leq r < b$:

$$\underbrace{234}_{a} = \underbrace{84}_{b} \times 2 + \underbrace{66}_{r_0}$$
$$\underbrace{84}_{b} = \underbrace{66}_{r_0} \times 1 + \underbrace{18}_{r_1}$$
$$\underbrace{66}_{r_0} = \underbrace{18}_{r_1} \times 3 + \underbrace{12}_{r_2}$$
$$\underbrace{18}_{r_1} = \underbrace{12}_{r_2} \times 1 + \underbrace{6}_{r_3}$$
$$\underbrace{12}_{r_2} = \underbrace{6}_{r_3} \times 2 + \underbrace{0}_{r_4}$$

Le reste r_4 est nul, donc l'algorithme s'arrête. $PGCD(234\,;\,84)$ est égal au dernier reste non nul r_3
Donc : $PGCD(234\,;\,84) = 6$

Démonstration :

- **1ère étape : montrons qu'il existe un avant dernier reste non nul et un dernier reste nul**

Les inégalités $b > r_0 > r_1 > \cdots > r_n > \cdots \geq 0$ montrent que (r_n) est une suite strictement décroissante d'entiers naturels. Or, il n'y a qu'un nombre fini d'entiers entre r_0 et 0. Donc cette suite est finie, c'est-à-dire qu'il existe un reste nul. Donc il existe un certain entier naturel k tel que $r_k \neq 0$ et $r_{k+1} = 0$.

[2] **Processus itératif :** processus répétitif

- **2ème étape : montrons que $PGCD(a\,,b) = PGCD(b\,,r_0)$.**

Considérons la relation de départ $a = bq_0 + r_0$. On en déduit que $r_0 = a - bq_0$.

La propriété fondamentale des diviseurs communs permet d'affirmer que :

Les diviseurs communs à $\boldsymbol{a}$ *et* $\boldsymbol{b}$ ***sont les mêmes*** *que les diviseurs communs* à $\boldsymbol{b}$ *et* $\boldsymbol{r_0}$

et $PGCD(a\,;b) = PGCD(b\,;r_0)$

- **3ème étape : montrons que $PGCD(a\,,b) = PGCD(r_k\,,0)$.**

On peut appliquer ce raisonnement à chaque égalité :

- $a = bq_0 + r_0$
- $b = r_0q_1 + r_1$
- $r_0 = r_1q_2 + r_2$
- .....
- $r_{k-2} = r_{k-1}\,q_k + r_k$
- $r_{k-1} = r_k\,q_{k+1} + r_{k+1}$

Si r_k est le dernier reste non nul (et donc $r_{k+1} = 0$), on a, en appliquant plusieurs fois la conséquence de **la propriété fondamentale des diviseurs communs :**

$$PGCD(a\,,b) = PGCD(b\,,r_0) = PGCD(r_0\,,r_1) = \cdots = PGCD(r_{k-2}\,,r_{k-1}) = PGCD(r_{k-1}\,,r_k)$$
$$= PGCD(r_k\,,r_{k+1}) = PGCD(r_k\,,0) = r_k$$

- Algorithme d'Euclide en langage naturel :

Déclaration des variables

A entier naturel

B entier naturel non nul

R entier naturel

Algorithme

A reçoit a

B reçoit b

R reçoit 1

Tant que $R \neq 0$ **faire**

R reçoit $A - B * PartEnt(A/B)$

A reçoit B

B reçoit R

Fin Tant que

Afficher « PGCD = », A

- Algorithme d'Euclide programmé sur TI82 - 83 :

```
PROGRAM:PGCD
:Prompt A,B
:1→R
:While R≠0
:A-B*PartEnt(A/B
)→R
:B→A
:R→B
:End
:Disp "PGCD=",A
```

2.2 Premier corollaire[3] de l'algorithme d'Euclide

Soit a et b deux entiers naturels non nuls. Notons $\boldsymbol{d = PGCD(a\,;b)}$.

L'ensemble des diviseurs communs à $\boldsymbol{a}$ et $\boldsymbol{b}$ est identique à l'ensemble des diviseurs de $\boldsymbol{PGCD(a\,;b)}$.

$$D(a) \cap D(b) = D(d)$$

Illustration :

Les diviseurs de $a = 234$ sont 1, 2, 3, 6, 9, 13, 18, 26, 39, 78, 117, 234 et leurs opposés.
Les diviseurs de $b = 84$ sont 1, 2, 3, 4, 6, 7, 12, 14, 21, 28, 42, 84 et leurs opposés.
Les diviseurs de $d = PGDC(234\,,84) = 6$ sont 1, 2, 3, 6 et leurs opposés.

Démonstration :

On reprend les divisions euclidiennes successives présentes dans l'algorithme d'Euclide :

- $a = bq_0 + \boldsymbol{r_0}$
- $b = \boldsymbol{r_0}q_1 + \boldsymbol{r_1}$
- $r_0 = \boldsymbol{r_1}q_2 + \boldsymbol{r_2}$
- .....
- $r_{k-2} = \boldsymbol{r_{k-1}}\, q_k + \boldsymbol{r_k}$
- $r_{k-1} = \boldsymbol{r_k}\, q_{k+1} + \boldsymbol{r_{k+1}}$

Si r_k est le dernier reste non nul (et donc $r_{k+1} = 0$), on a, en appliquant plusieurs fois **la propriété fondamentale des diviseurs communs** :

$$D(\boldsymbol{a}) \cap D(\boldsymbol{b}) = D(\boldsymbol{b}) \cap D(\boldsymbol{r_0}) = D(\boldsymbol{r_0}) \cap D(\boldsymbol{r_1}) = \cdots = D(\boldsymbol{r_{k-2}}) \cap D(\boldsymbol{r_{k-1}})$$
$$= D(\boldsymbol{r_{k-1}}) \cap D(\boldsymbol{r_k}) = D(\boldsymbol{r_k}) \cap D(\boldsymbol{0}) = D(\boldsymbol{r_k}) = D\big(PGDC(a\,;b)\big)$$

Conclusion : L'ensemble des diviseurs de $d = PGDC(a\,;b)$ est identique à l'ensemble des diviseurs communs à a et b

$$D\big(PGDC(a\,;b)\big) = D(a) \cap D(b)$$

Exemple 1 :

Déterminer tous les diviseurs communs à de $a = 345$ et $b = 1305$.

Réponse :
On cherche à la calculatrice $PGDC(345\,,1305)$
On trouve $d = PGDC(345\,,1305) = 15$
Les diviseurs de d sont donc $-15\,;\ -5\,;\ -3\,;\ -1\ ;1\ ;3\ ;5\ ;\ 15$
Conclusion : Les diviseurs communs à 345 et 1305 sont : $-15\,;\ -5\,;\ -3\,;\ -1\ ;1\ ;3\ ;5\ ;\ 15$

Exemple 2 :

$a = 234$ et $b = 84$ ont 2 parmi leurs diviseurs communs. Donc 2 divise $PGCD(234\,,84) = 6$

[3] **Corollaire :** Proposition qui se déduit immédiatement d'une proposition déjà démontrée.

2.3 Deuxième corollaire de l'algorithme d'Euclide

Soit a et b deux entiers relatifs non tous les deux nuls simultanément.

Pour tout $k \in \mathbb{N}^*$, $PGCD(ka\,, kb) = k \times PGCD(a\,, b)$

Exemple :

Soit $a = 234$ et $b = 84$.

$PGCD(234\,; 84) = 6$

Prenons $k = 5$.

$5 \times 234 = 1170$ et $5 \times 84 = 420$

$$PGCD(1170\,, 420) = 5 \times PGCD(234\,; 84)$$

$$PGCD(1170\,, 420) = 5 \times 6 = 30$$

Démonstration :

On pose $\boldsymbol{d = PGCD(a\,; b)}$ et $\boldsymbol{d' = PGCD(ka\,; kb)}$.

Pour montrer que $d' = k \times d$, on va montrer d'une part que kd divise d' (ce qui implique que $kd \leq d'$) et d'autre part que d' divise kd (ce qui implique que $d' \leq kd$). Donc, au final on aura démontré que $d' = kd$

1. **Montrons que $\boldsymbol{kd}$ divise $\boldsymbol{d'}$**

a et b sont deux entiers relatifs non tous les deux nuls simultanément et $k \in \mathbb{N}^*$.

$d = PGCD(a\,;\ b)$ divise à la fois a et b.

d divise a donc kd divise ka et d divise b donc kd divise kb

kd est donc un diviseur commun de ka et kb

D'après le premier corollaire de l'algorithme d'Euclide, l'ensemble des diviseurs communs de ka et kb est identique à l'ensemble des diviseurs de $PGCD(ka\,; kb) = d'$. **Donc $\boldsymbol{kd}$ est un diviseur de $\boldsymbol{d'}$.**

2. **Montrons que $\boldsymbol{d'}$ divise $\boldsymbol{kd}$**

On a vu dans la partie 1. Que **$\boldsymbol{kd}$ divise $\boldsymbol{d'}$ ce qui peut se traduire** :

Il existe un entier relatif k' tel $k'kd = d'$

$d' = PGCD(ka\,;\ kb)$ divise à la fois ka et kb.

En remplaçant $k'kd$ par d' , on peut donc dire que **$\boldsymbol{k'kd}$ divise à la fois $\boldsymbol{ka}$ et $\boldsymbol{kb}$.**

D'où :

$\boldsymbol{k'd}$ divise à la fois $\boldsymbol{a}$ et $\boldsymbol{b}$.

D'après le premier corollaire de l'algorithme d'Euclide, l'ensemble des diviseurs communs de a et b est identique à l'ensemble des diviseurs de $PGCD(a\,; b) = d$. Donc $k'd$ est un diviseur de d.

D'où :

$\boldsymbol{kk'd}$ est un diviseur de $\boldsymbol{dk}$

En remplaçant $k'kd = d'$ on peut donc déduire que **$\boldsymbol{d'}$ est un diviseur de $\boldsymbol{kd}$.**

Conclusion :

$$\boldsymbol{d' = kd} \qquad \textbf{c'est-à-dire} \qquad PGCD(\boldsymbol{k}a\,; \boldsymbol{k}b) = \boldsymbol{k}\, PGCD(a\,; b)$$

3 Théorème de Bézout[4]

3.1 Nombres premiers entre eux

Définition :

On dit que deux entiers relatifs *non nuls* a et b sont premiers entre eux (ou « étrangers ») lorsque leur PGCD est égal à 1.

Remarques :

a et b sont non nuls, alors :

- Les fractions $\frac{a}{b}$ et $\frac{b}{a}$ sont irréductibles lorsque a et b sont premiers entre eux.
- Si a et b ne sont pas premiers entre eux, alors on réduit ces fractions en divisant le numérateur et le dénominateur par $PGCD(a\,,b)$.

Exemple :

Les fractions $\frac{7}{234}$ et $\frac{13}{84}$ sont irréductibles car $PGCD(7\,,234)=1$ et $PGCD(13\,,84)=1$

Propriété

Soit a et b deux entiers naturels non nuls. On note $d=PGCD(a\,;b)$
Soit les entiers a' et b' tels que :

$$\begin{cases} a'=\dfrac{a}{d} \\ b'=\dfrac{b}{d} \end{cases}$$

Alors a' et b' sont premiers entre eux.

Démonstration :

d divise a et b. Donc il existe deux entiers a' et b' dans $\mathbb{Z}$ tels que $da'=a$ et $db'=b$.
Or en utilisant le deuxième corollaire de l'algorithme d'Euclide,

$$PGCD(a'd\ ;\ b'd)=d\ PGCD(a';b')$$

Donc $PGCD(a\ ;\ b)=d\ PGCD(a';b')$

$$\frac{PGCD(a\ ;\ b)}{d}=\ PGCD(a';b')$$

$$1=\ PGCD(a';b')$$

Conclusion :

a' et b' sont premiers entre eux.

Exemple :

Soit $a=234$ et $b=84$. $d=6$

$$a'=\frac{234}{6}=39$$

$$b'=\frac{84}{6}=14$$

$PGCD(39\,,14)=1$
39 et 14 sont premiers entre eux.

[4] **Etienne BEZOUT :** Mathématicien français 1730 – 1783. Auteur d'une théorie générale des équations algébriques (équations de la forme $P(x)=0$ où P est un polynôme).

3.2 Enoncé du théorème de Bézout

On note a b u v des entiers relatifs.

$$\mathbf{1 = PGCD(a,b) \quad \Leftrightarrow \quad au + bv = 1 \quad a\ des\ solutions\ (u,v)\ dans\ Z \times Z}$$

Ou encore :

$$\boldsymbol{a\ et\ b\ sont\ premiers\ entre\ eux \Leftrightarrow au + bv = 1 \quad a\ des\ solutions\ (u,v)\ dans\ Z \times Z}$$

Démonstration :

1. Démonstration de la proposition directe :

$$1 = PGCD(a,b) \quad \Longrightarrow \quad au + bv = 1 \quad a\ des\ solutions\ (u,v)$$

- **Si** $1 = PGDC(a\ ,b)$ alors au moins un des deux entiers a et b est non nul. Appelons a l'entier non nul.

a et b étant donnés, notons E l'ensemble des entiers $au + bv$. L'ensemble $\boldsymbol{E}$ **n'est pas vide** et il **contient au moins un entier strictement positif** (l'entier a qui correspond au couple $(u\ ;v) = (1\ ;0)$ ou l'entier – a qui correspond au couple $(u\ ;v) = (-1\ ;0)$).

Notons $\boldsymbol{\delta}$ **le plus petit des entiers strictement positifs** contenus dans l'ensemble E.

Il existe donc au moins **un couple d'entiers relatifs particulier** $(\boldsymbol{u_0}\ ;\boldsymbol{v_0})$ tel que $au_0 + bv_0 = \delta$.

- Ecrivons la relation de la division euclidienne de a par δ :

$$\begin{cases} a = \delta q + r \\ 0 \leq r < \delta \end{cases}$$

- Montrons que $r \in E$

$r = a - \delta q$

Or, $au_0 + bv_0 = \delta$

donc

$r = a - (au_0 + bv_0)q$

$r = a - aqu_0 - bqv_0$

$r = a(\mathbf{1} - \boldsymbol{qu_0}) + b(-\boldsymbol{qv_0})$

r est une combinaison linéaire entière de a et b de la forme $\boldsymbol{am} + \boldsymbol{bn}$ (il suffit de poser $m = (\mathbf{1} - \boldsymbol{qu_0})$ et $n = -\boldsymbol{qv_0}$ donc $r \in E$.

- Montrons que δ divise a

La condition $0 \leq r < \delta$ dans la division euclidienne de a par δ donne deux cas :

1er cas : $0 < r < \delta$

r est de la forme « $am + bn$ » et $r \neq 0$ donc $r \in E$. Mais il y a une contradiction entre $r \in E$ et $r < \delta$ (r ne peut pas être à la fois dans un ensemble et être strictement inférieur à son plus petit élément strictement positif).

2ème cas : $r = 0$ C'est la seule possibilité restante. Elle est donc vraie.

Conclusion : $r = 0$. Donc δ est un diviseur de a.

- De la même façon, en écrivant la relation de la division euclidienne de b par δ et en montrant que le reste ne peut être que nul, on montre que δ divise b.

- Concluons que $\delta = 1$

δ est donc un diviseur commun de a et b. Or a et b sont premiers entre eux et n'ont donc que deux diviseurs communs 1 et -1 . Comme δ est strictement positif, on a donc $\delta = 1$

Conclusion : **Si** $1 = PGDC(a\,,b)$ alors il existe donc au moins **un couple d'entiers relatifs particulier** $(\boldsymbol{u_0}\,;\boldsymbol{v_0})$ tel que $au_0 + bv_0 = 1$.

2. Démonstration de la proposition réciproque :

$$au\ +\ bv\ =\ 1\quad a\ des\ solutions\ (u,v) \Longrightarrow\quad 1 = PGCD(a,b)$$

S**'il** existe au moins un couple d'entiers relatifs $(u_0\,, v_0)$ tel que $au_0 + bv_0 = 1$ alors, puisque tout diviseur commun à a et b divise la combinaison linéaire $au_0 + bv_0 = 1$, alors tout diviseur commun à a et b divise 1.

Donc tout diviseur commun à a et b est dans l'ensemble $\{-1\,;1\}$.

D'où $PGDC(a\,;b) = 1$.

Conclusion : **S'il** existe au moins **un couple d'entiers relatifs particulier** $(\boldsymbol{u_0}\,;\boldsymbol{v_0})$ tel que $au_0 + bv_0 = 1$ alors $1 = PGDC(a\,,b)$

Exemple 1 :

Peut-on trouver un couple (au moins) d'entiers relatifs $(\boldsymbol{u},\boldsymbol{v})$ tel que $\boldsymbol{16u + 25v = 1}$

Réponse : $a = 16$ et $b = 25$ sont premiers entre eux. Donc, d'après le théorème de Bézout, il existe au moins un couple d'entiers relatifs (u,v) tel que $16u + 25v = 1$

Par exemple on trouve $(11,-7);\ (-14,9);\ (36,-23);\ (61,-39);$ … comme solutions.

Exemple 2 :

Peut-on trouver un couple (au moins) d'entiers relatifs $(\boldsymbol{u},\boldsymbol{v})$ tel que $\boldsymbol{4u + 10v = 1}$

Réponse : $a = 4$ et $b = 10$ ne sont pas premiers entre eux puisque $PGCD(4\,;10) \neq 1$. Donc, d'après le théorème de Bézout, la réponse est non.

Exemple 3 :

Soit $\boldsymbol{u}$ et $\boldsymbol{v}$ deux entiers relatifs. Sachant qu'il existe un couple (au moins) d'entiers relatifs $(\boldsymbol{x},\boldsymbol{y})$ tel que $\boldsymbol{(4xu - xy)u + (vy^2)v^2 = 1}$, que peut-on dire de $\boldsymbol{u}$ et $\boldsymbol{v^2}$?

Réponse : x, y, u et v sont des entiers relatifs. Donc $4xu - xy$ et vy^2 sont des entiers relatifs. Donc, d'après le théorème de Bézout, les entiers u et v^2 sont premiers entre eux.

Exemple 4 :

Montrer que pour tout $\boldsymbol{n} \in \mathbb{Z}$, $\boldsymbol{a = 2n + 1}$ et $\boldsymbol{b = 3n + 1}$ sont premiers entre eux.

Réponse : Comme la démonstration doit être faite quel que soit $n \in \mathbb{N}$, on cherche une combinaison linéaire qui élimine n :

$(2n + 1)(3) + (3n + 1)(-2) = 6n + 3 - 6n - 2.$

$\underline{(2n + 1)(3) + (3n + 1)(-2) = 1}$

D'après le théorème de Bézout, comme il existe au moins un couple d'entiers relatifs non nuls $(u\,, v)$ tel que $(2n + 1)u + (3n + 1)v = 1$ alors $= 2n + 1$ et $b = 3n + 1$ sont premiers entre eux $\forall n \in \mathbb{Z}$.

3.3 Corollaire du théorème de Bézout

On note $a\ b\ u\ v$ des entiers relatifs non nuls quelconques.

$$\boldsymbol{d = PGCD(a,b) \quad \Rightarrow \quad au\ +\ bv\ = d \quad a\ des\ solutions\ (u,v)}$$

⚠ **La réciproque** $au\ +\ bv\ = d \quad a\ des\ solutions\ (u,v) \quad \Rightarrow \quad d = PGCD(a,b)$ **est fausse**

Mais $\boldsymbol{d = PGCD(a,b) \quad \Leftrightarrow \quad au\ +\ bv\ = k \times d;\ \ k \in \mathbb{Z} \quad a\ des\ solutions\ (u,v)}$ **est vraie**

L'égalité $\boldsymbol{au + bv = PGCD(a\ ,b)}$ est appelée « identité de Bézout ».

Exemple :

Soit $a = 234, b = 84.\ PGCD(234\ ,84) = 6$

$\boldsymbol{234u + 84v = 6}$ est une identité de Bézout. Alors elle a des solutions comme par exemple :

$(u\ ,v) = (-5, 14)$, ou $(u\ ,v) = (79, -220)$ etc. Mais $\boldsymbol{234u + 84v = 12}$ a aussi des solutions.

Démonstration :

1. Démonstration de la proposition directe :

$$d = PGCD(a,b) \quad \Longrightarrow \quad au\ +\ bv\ =\ d \quad a\ \ des\ solutions\ (u,v)$$

- **Si** $d = PGDC(a\ ,b)$ alors au moins un des deux entiers a et b est non nul. Appelons a l'entier non nul.

Notons a' et b' les entiers définis par

$$a' = \frac{a}{d} \quad \text{et} \quad b' = \frac{b}{d}$$

a' est non nul. De plus, d'après la propriété vue au §3.1, a' et b' sont premiers entre eux.

Donc si $d = PGDC(a\ ,b)$, alors l'équation $au\ +\ bv\ =\ d$ équivaut successivement à :

$$\frac{au\ +\ bv}{d} = 1$$

$$\frac{au}{d} + \frac{bv}{d} = 1$$

$a'u + b'v = 1$ avec a' et b' premiers entre eux

D'après le théorème de Bézout, cette équation a des solutions (u, v) .

2. Démonstration que la proposition réciproque est fausse :

Si $au\ +\ bv\ =\ d \quad a\ \ des\ solutions\ (u,v)$ alors d peut ne pas être le $PGCD(a\ ;\ b)$.

Contre-exemple :

L'équation $234u\ +\ 84v\ =\ 66 \quad a\ \ des\ solutions\ (u,v)$ (par exemple $(u\ ;v) = (1\ ;-2)$) alors que 66 **n'est pas le PGCD** de $a = 234$ et $b = 84$.

Dans le paragraphe suivant, on montre que d peut être **tout multiple du $\boldsymbol{PGCD(a\ ;\ b)}$**

Conclusion :

Si a et b sont deux entiers relatifs non nuls, alors l'équation $\boldsymbol{au + bv = d}$ avec $d = PGCD(a\ ,b)$ a au moins un couple d'entiers relatifs u et v solution

3.4 CNS[5] pour qu'une équation diophantienne $ax + by = c$ ait des solutions

On appelle équation diophantienne[6] une équation dont les coefficients sont des entiers relatifs et dont on cherche uniquement des solutions entières relatives. L'équation $ax + by = c$ est une équation diophantienne du type linéaire à deux inconnues.

L'équation $ax + by = c$	où a, b, c sont des entiers relatifs non nuls	a des solutions $(x\,;y)$ entières relatives	**si et seulement si**	$\underline{c = kd}$ avec $k \in \mathbb{Z}$ et $\underline{d = PGDC(a\,,b)}$.

Exemples :

Dans le cas de $a = 234$ et $b = 84$, on a $d = PGDC(a\,,b) = 6$

- Les équations $ax + by = 6$, $ax + by = 12$, $ax + by = -18$ … de manière générale $ax + by = 6k$, $k \in \mathbb{Z}$ ont toutes une infinité de couples de solutions entières $(x\,;y)$.
- Les équations $ax + by = 1$, $ax + by = 2$, $ax + by = -3$ … de manière générale $ax + by = c$ avec $c \neq 6k$, $k \in \mathbb{Z}$ n'ont aucun couple de solutions entières $(x\,;y)$.

Démonstration :

On note d le $PGCD(a\,,b)$

1ère étape : démontrons que $ax + by$ est toujours un multiple de d

Si $(x\,;y)$ est un couple d'entiers relatifs quelconques, puisque a est un multiple de d et b est un multiple de d **alors** $ax + by = (p \times d)x + (q \times d)y$ avec p et q entiers relatifs.

$ax + by = (px + qy)d$. Comme $px + qy$ est entier relatif **alors** $\underline{ax + by}$ est un multiple de $\underline{d}$.

2ème étape : démontrons que $ax + by = kd$ a toujours des solutions $(x\,;y)$ entières relatives.

D'après l'identité de Bézout, il existe au moins un couple d'entiers $(u\,,v)$ tels que $au + bv = d$ c'est-à-dire tels que $k(au + bv) = kd$.

$a(uk) + b(vk) = kd$.

L'identité de Bézout permet d'affirmer que l'équation $ax + by = kd$ a toujours des solutions

Ce sont tous les couples $(x\,;y) = (uk\,;kv)$ multiples d'un couple $(u\,,v)$ solution de $ax + by = d$

Conclusion :

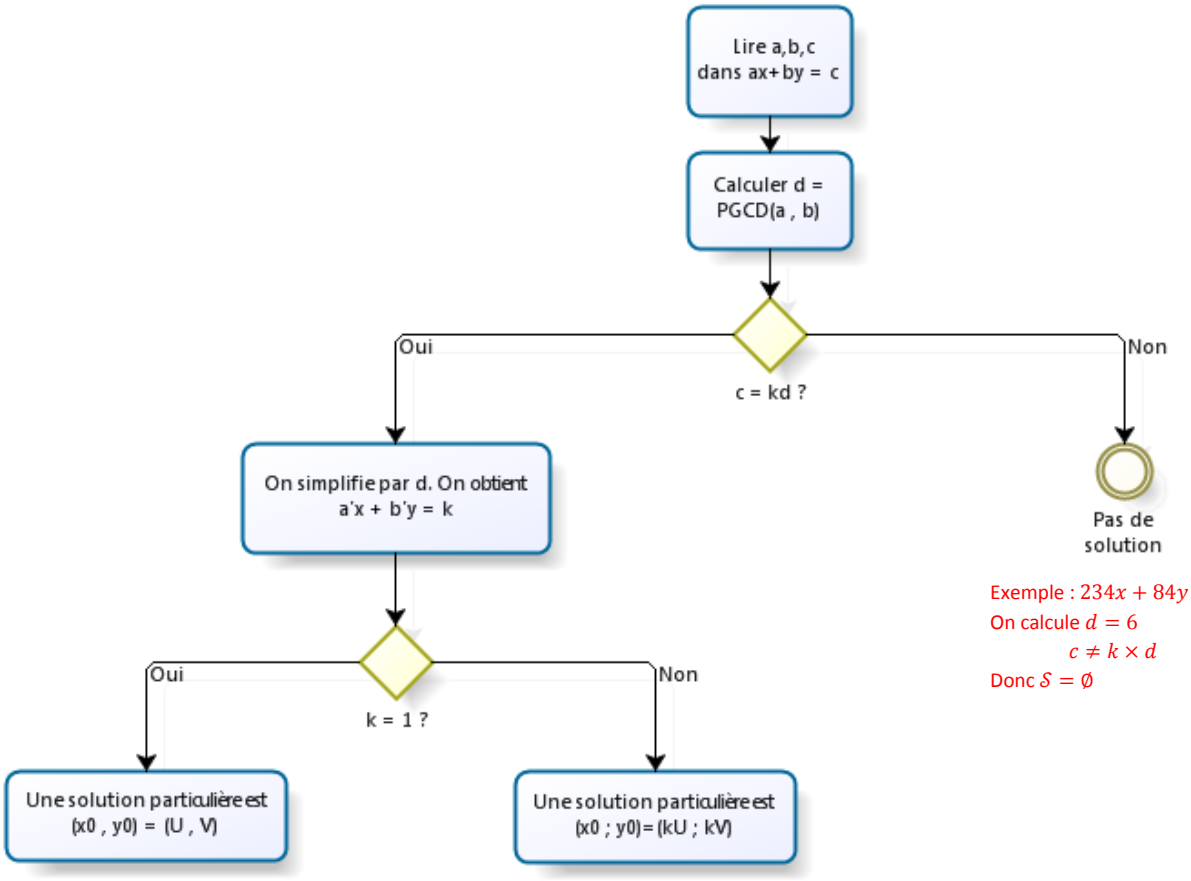
Les solutions $(x\,;y)$ entières relatives existent **si et seulement si** l'équation est du type $ax + by = c$ avec :

- $\underline{Soit\ c = PGCD(a\,,b)}$
- $\underline{Soit\ c}$ est un multiple de $\underline{PGCD(a\,;b).}$

[5] CNS : Condition Nécessaire et Suffisante

[6] **Diophante d'Alexandrie :** mathématicien grec (3ème siècle après Jésus Christ). Son ouvrage « *Arithmétiques* » constituent l'apogée de l'algèbre grecque (algèbre : partie des mathématiques traitant des équations et des opérations).

3.5 Détermination d'une solution particulière $(x_0 ; y_0)$ de $ax + by = c$



Exemple : $234x + 84y = 5$
On calcule $d = 6$
$c \neq k \times d$
Donc $\mathcal{S} = \emptyset$

Exemple : $234x + 84y = 6$

- On calcule $d = 6$
- On a bien $c = kd$
- On divise les membres par d

$39x + 14y = 1$
L'algorithme BEZOUT pour $a = 39$ *et* $b = 14$
donne $U = -5$ et $V = 14$

- Puisque $k = 1$

alors $(x_0; y_0) = (-5 ; 14)$

Exemple : $234x + 84y = 12$

- On calcule $d = 6$
- On a bien $c = kd$
- On divise les membres par d

$39x + 14y = 2$
L'algorithme BEZOUT pour $a = 39$ *et* $b = 14$
donne $U = -5$ et $V = 14$

- Puisque $k = 2$

alors $(x_0; y_0) = (-10 ; 28)$

Remarque : Comment trouver manuellement des valeurs des coefficients de Bézout U et V ?
Soit à trouver des valeurs de u et v pour l'identité de Bézout suivante $39u + 14v = 1$
39 et 14 sont premiers entre eux, donc c'est une identité de Bézout et il y a des solutions (u , v)

- On pose $a = 39$ et $b = 14$ et on écrit la succession des divisions euclidiennes en commençant par $a \div b$ jusqu'au dernier reste non nul $r_k = 1$
- On exprime les restes comme combinaisons linéaires de a et b à chaque ligne :

Avec des chiffres	Avec des lettres	**Expression du reste $r(a , b)$**
$39 = 14 \times 2 + \mathbf{11}$	$a = 2b + \mathbf{11}$	$\mathbf{11} = a - 2b$
$14 = \mathbf{11} \times 1 + \mathbf{3}$	$b = (\boldsymbol{a - 2b}) \times 1 + \mathbf{3}$	$\mathbf{3} = -a + 3b$
$11 = \mathbf{3} \times 3 + \mathbf{2}$	$(a - 2b) = (\boldsymbol{-a + 3b}) \times 3 + \mathbf{2}$	$\mathbf{2} = 4a - 11b$
$3 = \mathbf{2} \times 1 + \mathbf{1}$	$(-a + 3b) = (\boldsymbol{4a - 11b}) \times 1 + \mathbf{1}$	$-5a + 14b = 1$

- La dernière combinaison linéaire de a et b est égale à 1. Elle donne une solution $(u ; v)$

La recherche des coefficients de Bézout peut être faite à l'aide l'algorithme « BEZOUT » suivant :

Déclaration des variables :

A, B, C,D,E,F, Q, R, S, T, U, V, X, Y entiers relatifs

Algorithme :

début

Saisir A, B

C reçoit $|A|$ *** Cette instruction permet le fonctionnement correct si A < 0 ***

D reçoit $|B|$ *** Cette instruction permet le fonctionnement correct si B < 0 ***

E reçoit A/C

F reçoit B/D

U reçoit 1

X reçoit 0

V reçoit 0

Y reçoit 1

R reçoit 1

Tant que $R \neq 0$ **faire**

Q reçoit $partEnt(C/D)$

R reçoit $C - D * Q$

C reçoit D

B reçoit R

S reçoit $U - X * Q$

U reçoit X

X reçoit S

T reçoit $V - Y * Q$

V reçoit Y

Y reçoit T

FinTant que

$afficher$ "PGCD=", C.

U reçoit $U * E$ *** Cette instruction rétablit la bonne valeur de U si A < 0 ***

V reçoit $V * F$ *** Cette instruction rétablit la bonne valeur de V si B < 0 ***

$afficher$ "U=", U.

$afficher$ "V=", V.

Fin

```
PROGRAM:BEZOUT
:Prompt A,B
:abs(A)→C
:abs(B)→D
:A/C→E
:B/D→F
:1→U
:0→X
:0→V
:1→Y
:1→R
:While R≠0
:partEnt(C/D)→Q
:C-D*Q→R
:D→C
:R→D
:U-X*Q→S
:X→U
:S→X
:V-Y*Q→T
:Y→V
:T→Y
:End
:Disp "PGCD=",C
:U*E→U
:V*F→V
:Disp "U=",U
:Disp "V=",V
```

4 Théorème de Gauss

4.1 Enoncé du théorème de Gauss[7]

Soit a, b, et c trois entiers relatifs non nuls.

Si $\begin{cases} a \text{ divise } bc \\ a \text{ et } b \textit{ sont premiers entre eux} \end{cases}$ **alors** ***a* divise *c***.

Exemple :

$\begin{cases} 2 \text{ divise } 3 \times 4 \\ 2 \text{ et } 3 \text{ premiers entre eux} \end{cases}$ **alors** 2 divise 4.

Démonstration :

Pour démontrer le théorème de Gauss, on va utiliser le théorème de Bézout :

- a et b sont premiers entre eux équivaut à

$$au + bv = 1 \text{ a des couples d'entiers relatifs } (u\,;v) \text{ solutions.}$$

- On multiplie les deux membres de cette égalité par c :

$$auc + bvc = c \text{ a des couples } (u\,;v) \text{ solutions.}$$

- Comme a divise bc alors il existe un entier relatif k tel que $ak = bc$ et on remplace bc

L'égalité devient :

$$auc + akv = c \text{ a des couples } (u\,;v) \text{ solutions.}$$
$$(uc + kv)a = c \text{ a des couples } (u\,;v) \text{ solutions.}$$

$uc + kv \in \mathbb{Z}$ donc ***a* divise *c***.

4.2 Première corollaire du théorème de Gauss

Soit a, b, et c trois entiers relatifs non nuls.

Si $\begin{cases} a \text{ divise } c \\ b \text{ divise } c \\ a \text{ et } b \textit{ sont premiers entre eux} \end{cases}$ **alors** ***ab* divise *c***.

Exemple :

$\begin{cases} 2 \text{ divise } 12 \\ 3 \text{ divise } 12 \\ 2 \text{ et } 3 \text{ sont premiers entre eux} \end{cases}$ **alors** 2×3 divise 12.

Contre-exemple :

$\begin{cases} 4 \text{ divise } 12 \\ 6 \text{ divise } 12 \\ \ldots \end{cases}$ **alors** 4×6 divise 12 est faux (car il manque l'hypothèse a et b sont premiers entre eux)

[7] **Karl Friedrich Gauss** astronome, mathématicien et physicien allemand (Brunswick 1777 - Göttingen 1855), auteur d'importants travaux en mécanique céleste, en géodésie, sur le magnétisme, l'électromagnétisme et l'optique. Sa conception moderne de la nature abstraite des mathématiques lui permit d'étendre le champ de la théorie des nombres.

Démonstration :

- ***1ère étape : on traduit*** $\begin{cases} \boldsymbol{a} \textbf{ divise } \boldsymbol{c} \\ \boldsymbol{b} \textbf{ divise } \boldsymbol{c} \end{cases}$

$\begin{cases} a \text{ divise } c \\ b \text{ divise } c \end{cases}$ donc il existe $k \in \mathbb{Z}$ et $l \in \mathbb{Z}$ tels que $\begin{cases} ak = c \\ bl = c \end{cases}$

- ***2ème étape : on déduit que b divise ak***

$ak = bl$ avec $l \in \mathbb{Z}$ donc b divise ak

- ***3ème étape : Utilisation du théorème de Gauss***

$\begin{cases} b \text{ divise } a \times k \\ b \text{ et } a \text{ sont premiers entre eux} \end{cases}$ **alors** b divise k.

- ***4ème étape : on traduit b divise k***

b divise k donc il existe $k' \in \mathbb{Z}$ tel que $bk' = k$

Conclusion : $ak = c$ s'écrit donc $abk' = c$ ce qui montre que ab divise c.

4.3 Deuxième corolaire du théorème de Gauss

Si un nombre premier p divise **un produit ab** alors p divise au moins l'un des facteurs a ou b

Exemples :

5 divise 7×35. Ici 5 divise $b = 35$.

5 divise 15×35. Ici 5 divise $a = 15$ et $b = 35$.

Démonstration :

Soit p un nombre premier divisant le produit ab.

Si p divise a, la conclusion est assurée.

Si p ne divise pas a, puisque p est premier, alors a et p sont premiers entre eux.

Si $\begin{cases} p \text{ divise } ab \\ p \text{ et } a \textit{ sont premiers entre eux} \end{cases}$ **alors d'après le théorème de Gauss $\boldsymbol{p}$ divise $\boldsymbol{b}$**.

4.4 Troisième corolaire du théorème de Gauss

Si un nombre **premier p** divise **un produit de nombres premiers ab** alors $p = a$ ou $p = b$

Exemples :

5 divise 7×5. Ici $5 = b$.

5 divise 5×5. Ici $5 = a = b$

Démonstration :

Soit les nombres premiers a, b, p.

On suppose que p divise ab.

1er cas : $p = a$. Donc p divise a.

2ème cas : $p \neq a$. Donc a et p sont donc premiers entre eux.

Si $\begin{cases} p \text{ divise } ab \\ p \text{ et } a \text{ sont premiers entre eux} \end{cases}$ **alors d'après le théorème de Gauss** **p divise b**.

Et comme p et b sont premiers, alors $p = b$.

4.5 Quatrième corolaire du théorème de Gauss

Soit p, a, b des entiers relatifs non nuls.

$\begin{cases} p \text{ et } a \text{ sont premiers entre eux} \\ p \text{ et } b \text{ sont premiers entre eux} \end{cases}$	**équivaut à**	p et $(a \times b)$ sont premiers entre eux

Exemple :

$\begin{cases} 2 \text{ et } 3 \text{ sont premiers entre eux} \\ 2 \text{ et } 5 \text{ sont premiers entre eux} \end{cases}$ **équivaut à** 2 est premier avec $3 \times 5 = 15$.

Démonstration :

1. Démonstration de la proposition directe :

$$\begin{cases} p \text{ et } a \text{ sont premiers entre eux} \\ p \text{ et } b \text{ sont premiers entre eux} \end{cases} \Longrightarrow \quad p \text{ et } (a \times b) \text{ sont premiers entre eux}$$

Soit p, a, b trois entiers relatifs tels que $\begin{cases} p \text{ et } a \text{ sont premiers entre eux} \\ p \text{ et } b \text{ sont premiers entre eux} \end{cases}$

Supposons que p et ab aient un diviseur commun entier naturel d. Montrons qu'alors $d = 1$.

d divise p donc d divise ap

Comme on suppose que d divise aussi ab et on sait (1er corollaire de l'algorithme d'Euclide) que l'ensemble des diviseurs communs à ap et ab est identique à l'ensemble des diviseurs communs de $PGCD(ap\,;ab)$ **alors d divise $PGCD(ap\,;ab)$.**

Comme $PGCD(ap\,;ab) = a \times PGCD(p\,;b)$ alors d divise $a \times PGCD(p\,;b)$

Dans les hypothèses, p et b sont premiers entre eux donc $PGCD(p\,;b) = 1$.

D'où d divise a

Comme d divise aussi p, alors d est un diviseur commun de a et p.

Dans les hypothèses**, p et a sont premiers entre eux donc $d = 1$.**

Le diviseur commun de p et ab est 1 .

Conclusion : p et $(a \times b)$ sont premiers entre eux.

2. Démonstration de la proposition réciproque :

$$p \text{ et } (a \times b) \text{ sont premiers entre eux } \Longrightarrow \begin{cases} p \text{ et } a \text{ sont premiers entre eux} \\ p \text{ et } b \text{ sont premiers entre eux} \end{cases}$$

Soit un nombre entier relatif p premier avec le produit d'entiers relatifs ab.

Supposons que p et a aient un diviseur commun **entier naturel d.**

Alors d divise p et ab. Comme on suppose ici que p et $(a \times b)$ sont premiers entre eux, alors $d = 1$.

Comme le diviseur commun entier naturel d de p et a est , on déduit que p et a sont premiers entre eux.

En supposons que p et b aient un diviseur commun **entier naturel d, on démontre de même que p et b sont premiers entre eux.**

Conclusion : $\begin{cases} p \text{ et } a \text{ sont premiers entre eux} \\ p \text{ et } b \text{ sont premiers entre eux} \end{cases}$.

Exemple :
22 est premier avec 57 et 35 donc 22 est premier avec $57 \times 35 = 1995$.
Mais aussi :
22 est premier avec 1995 donc 22 est premier avec chacun des facteurs 57 et 35.

4.6 Utilisation du théorème de Gauss pour déterminer l'ensemble des couples de solutions entières $(x\,;y)$ d'une équation diophantienne du type $ax + by = 0$

Exemple : Résoudre dans $\mathbb{Z} \times \mathbb{Z}$ l'équation $42x + 30y = 0$

1ère étape : on transforme l'équation en $p \times x = (qy)$ avec p et q premiers entre eux
Soit $a = 42$ et $b = 30$. $PGCD(42\,,30) = 6$

$$\frac{42x + 30y}{6} = \frac{0}{6}$$

$$\mathbf{7x + 5y = 0}$$

$$7 \times x = (-5y)$$

2ème étape : Recherche de la forme des couples solution $(x\,;y)$ à l'aide du théorème de Gauss

- **Si** $(x\,;y)$ vérifie $7 \times x = (-5y)$ alors 7 divise $-5y$
- $\begin{cases} 7 \text{ divise } -5y \\ 7 \text{ et } -5 \text{ sont premiers entre eux} \end{cases}$ **alors d'après le théorème de Gauss** 7 divise y.
- 7 divise y s'écrit : il existe $k \in \mathbb{Z}$ tel que $7k = y$
- En reportant dans l'équation $7 \times x = (-5y)$, on trouve $x = -5k$
- **Alors** les couples solutions sont de la forme $(-5k\,;7k)$ où $k \in \mathbb{Z}$.

3ème étape : Réciproquement on vérifie que tout couple $(-5k\,;7k)$ où $k \in \mathbb{Z}$ est solution
$42x + 30y = 42(-5k) + 30(7k) = -210k + 210k = 0$ pour tout entier relatif k

Conclusion : L'ensemble des solutions est $\mathcal{S} = \{(-5k\,;7k);\ k \text{ décrit } \mathbb{Z}\}$

Par exemple, les couples $(5\,;-7)$, $(0\,;0)$, $(-5\,;7)$, $(-10\,;14)$, $(-15\,;21)$ … sont des solutions.

4.7 Utilisation du théorème de Gauss pour déterminer l'ensemble des couples de solutions $(x\,;y)$ d'une équation du type $ax + by = c$

Rappel :

Les solutions $(x\,;y)$ entières existent **si et seulement si** l'équation est du type $ax + by = kd$ avec :

$$d = PGCD(a\,,b)$$

On a vu au paragraphe 3.4 qu'on pouvait trouver un couple de solutions particulières (x_0, y_0) en mettant l'équation sous la forme $a'x + b'y = k$ avec a' et b' premiers entre eux, puis en trouvant des coefficients de Bézout $(u\,;v)$ de l'identité de Bézout $a'u + b'v = 1$.

Exemple 1 :

Soit l'équation $\mathbf{6x + 5y = 1}$ **(E)**

1) Déterminer une solution particulière de (E)
2) Résoudre dans $\mathbb{Z} \times \mathbb{Z}$ l'équation (E)

Réponse :

1) (E) est une équation du type $au + bv = 1$ avec $a = 6$ et $b = 5$. On vérifie que a et b sont premiers entre eux. Donc, d'après le théorème de Bézout, cette équation admet des couples $(x\,,y)$ solution. A la calculatrice on trouve $u = 1\,,\ v = -1$.

   Donc une solution particulière de $\mathbf{6x + 5y = 1}$ est : $(x_0\,,y_0) = (1\,,-1)$

2) *L'existence de cette solution particulière permet de revenir à une équation sans second membre comme dans l'exemple du paragraphe 4.6 précédent.*

   On soustrait membre à membre $6x + 5y = 1$ (E) et $6x_0 + 5y_0 = 1$

   $6x + 5y - \big(6(1) + 5(-1)\big) = 1 - 1$

   $\mathbf{6(x-1) + 5(y+1) = 0}$

1. ***Transformation de l'équation en $p \times X = (qY)$ avec p et q premiers entre eux***

   Soit $a = 6$ et $b = 5$. $PGCD(6\,,5) = 1$

   $6 \times (x-1) = -5(y+1)$

2. ***Recherche de la forme des couples solution à l'aide du théorème de Gauss***

- **Si** $(x-1\,;y+1)$ vérifie $6 \times (x-1) = -5(y+1)$ alors 6 divise $-5(y+1)$
- $\begin{cases} 6 \text{ divise } -5(y+1) \\ 6 \text{ et } -5 \text{ sont premiers entre eux} \end{cases}$ **donc d'après le théorème de Gauss** 6 divise $(y+1)$.
- 6 divise $(y+1)$ s'écrit : il existe $k \in \mathbb{Z}$ tel que $6k = y + 1$
- En reportant dans l'équation $\mathbf{6 \times (x-1) + 5(y+1) = 0}$,
  on trouve $\mathbf{6(x-1) + 5(6k) = 0}$ c'est-à-dire $(x-1) + 5(k) = 0$ soit $x - 1 = -5k$
- **Alors** les couples $(x\,;y)$sont de la forme $(-5k+1\,;6k-1)$ où $k \in \mathbb{Z}$.

3. ***<u>Réciproquement on vérifie</u> que tout couple $(-5k+1\,;6k-1)$ où $k \in \mathbb{Z}$ est solution de l'équation*** $\mathbf{6x + 5y = 1}$ **(E)**

   $6(-5k+1) + 5(6k-1) = -30k + 6 + 30k - 5$

   $6(-5k+1) + 5(6k-1) = 1$ <u>pour tout entier relatif k.</u>

<u>Conclusion :</u> L'ensemble des solutions de l'équation (E) est $\mathcal{S} = \{(-5k+1\,;6k-1)\,;\ k \text{ décrit } \mathbb{Z}\}$

Par exemple, les couples $(6\,;-7)$, $(1\,;-1)$, $(-9\,;11)$, $(-14\,;17)$ … sont des solutions.

Exemple 2 :

Soit l'équation $\mathbf{6x + 5y = 3}$ **(E)**

1) Déterminer une solution particulière de (E)
2) Résoudre dans $\mathbb{Z} \times \mathbb{Z}$ l'équation (E)

Réponse :

1) (E) est une équation du type $au + bv = 3 \times 1$ avec $a = 6$ et $b = 5$. On vérifie que a et b sont premiers entre eux.

   Donc, (voir le schéma du § 3.5) on résout d'abord l'équation $\mathbf{6u + 5v = 1}$ D'après le théorème de Bézout, cette équation admet des couples $(u\,, v)$ solution. A la calculatrice on trouve $u_0 = 1$, $v_0 = -1$.

   Donc une solution particulière de $\mathbf{6x + 5y = 3}$ est : $(x_0\,, y_0) = (3\,, -3)$

2) *L'existence de cette solution particulière permet de revenir à une équation sans second membre comme dans l'exemple du paragraphe 4.7 précédent.*

On soustrait membre à membre $6x + 5y = 3$ (E) et $6x_0 + 5y_0 = 3$

$6x + 5y - \big(6(3) + 5(-3)\big) = 3 - 3$

$\mathbf{6(x - 3) + 5(y + 3) = 0}$

1. ***Transformation de l'équation en $p \times x = (qy)$ avec p et q premiers entre eux***

   Soit $a = 6$ et $b = 5$. $PGCD(6\,, 5) = 1$

   $6 \times (x - 3) = -5(y + 3)$

2. ***Recherche de la forme des couples solution à l'aide du théorème de Gauss***

- **Si** $(x - 3\,; y + 3)$ vérifie $6 \times (x - 3) = -5(y + 3)$ alors 6 divise $-5(y + 3)$
- $\begin{cases} 6 \text{ divise } -5(y+3) \\ 6 \text{ et } -5 \text{ sont premiers entre eux} \end{cases}$ **donc d'après le théorème de Gauss** 6 divise $(y + 3)$.
- 6 divise $(y + 3)$ s'écrit : il existe $k \in \mathbb{Z}$ tel que $6k = y + 3$
- En reportant dans l'équation $\mathbf{6 \times (x - 3) + 5(y + 3) = 0}$,
  on trouve $\mathbf{6(x - 3) + 5(6k) = 0}$ c'est-à-dire $(x - 3) + 5(k) = 0$ soit $x - 3 = -5k$
- **Alors** les couples $(x\,; y)$sont de la forme $(-5k + 3\,; 6k - 3)$ où $k \in \mathbb{Z}$.

3. ***<u>Réciproquement on vérifie</u> que tout couple $(-5k + 3\,; 6k - 3)$ où $k \in \mathbb{Z}$ est solution de l'équation*** $\mathbf{6x + 5y = 3}$ **(E)**

   $6(-5k + 3) + 5(6k - 3) = -30k + 18 + 30k - 15$

   $6(-5k + 3) + 5(6k - 3) = 3$ <u>pour tout entier relatif k.</u>

<u>Conclusion :</u> L'ensemble des solutions de l'équation (E) est $\mathcal{S} = \{(-5k + 3\,; 6k - 3)\,;\ k \text{ décrit } \mathbb{Z}\}$

Par exemple, les couples $(8\,; -9)$, $(3\,; -3)$, $(-7\,; 9)$, $(-12\,; 15)$ … sont des solutions.