# THÉORÈMES FONDAMENTAUX

Remarque : lorsqu'on parlera de *diviseurs*, il sera sous-entendu qu'il s'agit de diviseurs *positifs*.

## I Théorème de Bézout

### 1° Le théorème

Définition : Deux nombres sont premiers entre eux si leur seul diviseur commun est 1.

Autrement dit, deux nombres sont premiers entre eux si leur PGCD vaut 1.

Théorème : Soient $a$ et $b$ deux entiers naturels non nuls.

$a$ et $b$ premiers entre eux $\Leftrightarrow$ $\exists (u\,;v) \in \mathbb{Z}^2,\ au + bv = 1.$

Preuve : ($\Leftarrow$) Supposons qu'il existe $u$ et $v$ tels que $au + bv = 1$.

Soit $\Delta$ un diviseur commun à $a$ et $b$. On a $\Delta | a$ et $\Delta | b$ donc $\Delta | au + bv$.

Autrement dit, $\Delta | 1$ et donc $\Delta = 1$.

Le seul diviseur commun à $a$ et $b$ est donc 1 : $a$ et $b$ sont premiers entre eux.

($\Rightarrow$) Supposons que $a$ et $b$ sont premiers entre eux.

Soit $\mathcal{A}$ l'ensemble des nombres pouvant s'écrire $au + bv$ : $\mathcal{A} = \{au + bv, (u\,;v) \in \mathbb{Z}^2\}$

Avec $u = 1$ et $v = 0$, $au + bv = a$ donc $a \in \mathcal{A}$. Autrement dit, $\mathcal{A} \neq \emptyset$.

Notons $m$ le plus petit entier strictement positif de $\mathcal{A}$.

Il existe donc $(u_1\,;v_1) \in \mathbb{Z}^2$ tel que $m = au_1 + bv_1$.

Par ailleurs, la division euclidienne de $a$ par $m$ donne $a = mq + r$ avec $0 \leq r < m$.

Ainsi, $r = a - mq$

$= a - (au_1 + bv_1)q$

$= a - au_1q - bv_1q$

$= a(1 - u_1q) + b(-v_1q)$

Donc $r \in \mathcal{A}$.

Or, $r < m$ et $m$ est le plus petit élément strictement positif de $\mathcal{A}$ donc $r = 0$.

Autrement dit, $m | a$ ; et de même, on montre que $m | b$.

$m$ est donc un diviseur commun à $a$ et $b$.

Or, $a$ et $b$ sont premiers entre eux donc $m = 1$.

Par conséquent, il existe $(u_1\,;v_1) \in \mathbb{Z}^2$ tel que $au_1 + bv_1 = 1$.

Corollaire : Soient $a$ et $b$ deux entiers naturels non nuls.

Si $\Delta = \text{PGCD}(a\,;b)$ alors il existe deux entiers relatifs $u$ et $v$ tels que $\Delta = au + bv$.

Preuve : $\Delta$ est le PGCD de $(a\,;b)$ donc il existe donc deux entiers naturels $a'$ et $b'$ tels que $a = \Delta a'$, $b = \Delta b'$ et $\text{PGCD}(a'; b') = 1$.

D'après Bézout, il existe deux entiers relatifs $u$ et $v$ tels que $a'u + b'v = 1$.

D'où $\Delta(a'u + b'v) = \Delta \times 1$

$$\Delta a'u + \Delta b'v = \Delta$$

$$(\Delta a')u + (\Delta b')v = \Delta$$

**2° Mise en œuvre pratique**

Le théorème de Bézout nous assure de l'existence d'un couple $(u\,;v)$ mais comment peut-on le déterminer ?

⇨ Par remontée de l'algorithme d'Euclide

Ex : démontrer que 89 et 41 sont premiers entre eux puis déterminer une solution de l'équation $89x + 41y = 1$.

On utilise l'algorithme d'Euclide :

$$89 = 41 \times 2 + 7$$

$$41 = 7 \times 5 + 6$$

$$7 = 6 \times 1 + 1$$

Donc $\text{PGCD}(89\,;41) = 1$.

D'après la dernière égalité de l'algorithme d'Euclide, on a :

$$1 = 7 - 6$$

$$1 = 7 - (41 - 7 \times 5)$$

$$1 = 7 - 41 + 7 \times 5$$

$$1 = 7 \times 6 - 41$$

$$1 = (89 - 41 \times 2) \times 6 - 41$$

$$1 = 89 \times 6 - 41 \times 12 - 41$$

$$1 = 89 \times 6 - 41 \times 13$$

D'où $x = 6$ et $y = -13$.

Remarque : pour trouver non pas *une* mais *les* solutions de $89x + 41y = 1$, il faut attendre le II…

⇨ A l'aide de la calculatrice *(si on ne demande pas de faire explicitement les choses)*

Ex : On admet que PGCD$(113\,;59)=1$. Déterminer une solution de l'équation $113x+59y=1$.

BROUILLON

On a $113x+59y=1$

$59y=1-113x$

$y=\dfrac{1-113x}{59}$

On entre ça dans $f(x)$ ➔ table de valeurs ➔ on obtient $x=47$ et $y=-90$.

$113\times 47+59\times(-90)=5\,311-5\,310=1.$

Donc $x=47$ et $y=-90$ est une solution de l'équation.

**3° Application : le chiffrement affine**

Il s'agit d'une méthode élémentaire de cryptographie, mais trop simple à casser et donc quasi jamais utilisée. Mais c'est un bon exemple d'initiation qui permet de comprendre la place de l'arithmétique dans la cryptographie.

On commence par remplacer chaque lettre par son rang, en commençant généralement par 0 :

| A | B | C | D | E | F | G | H | I | J | K | L | M |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |

| N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

Le codage : on choisit deux entiers $a$ et $b$ comme clés. Chaque lettre est remplacée par son équivalent numérique $x$, lequel est ensuite chiffré en $y$ tel que $y\equiv ax+b\ \ [26]$

Ex : prenons la clé (7 ; 11) : on a donc la relation $y\equiv 7x+11\ \ [26]$

MATHS donne tout d'abord la séquence numérique 12 / 0 / 19 / 7 / 18

L'image de $x=12$ est $y=7\times 12+11$

$=95$

$\equiv 17\ \ [26]$

L'image de $x=0$ est $y=7\times 0+11$

$=11$

$\equiv 11\ \ [26]$

De même, l'image de 19 est 14, celle de 7 est 8 et celle de 18 est 7.

La séquence 12 / 0 / 19 / 7 / 18 devient alors 17 / 11 / 14 / 8 / 7, ce qui correspond à RLOIH.

Au final : MATHS ➔ 12 / 0 / 19 / 7 / 18 ➔ 17 / 11 / 14 / 8 / 7 ➔ RLOIH

Le décodage : il consiste à retrouver l'antécédent $x$ de $y$ sachant que $ax + b \equiv y \ \ [26]$

$ax + b = y$ donne sans problème $ax = y - b$ mais pour « simplifier » par $a$ il faut pouvoir trouver un coefficient $a'$ tel que $a \times a' \equiv 1 \ \ [26]$.

Autrement dit, $aa' = 1 + 26k$ et donc $aa' - 26k = 1$ : d'après le théorème de Bézout, ce n'est possible que si $a$ et 26 sont premiers entre eux. *(toutes les clés ne sont donc pas valides !)*

Ex : On dispose de la clé (7 ; 11) et on reçoit le message RLOIH.
Tout d'abord, RLOIH donne la séquence 17 / 11 / 14 / 8 / 7.

La relation liée à la clé (7 ; 11) est $y \equiv 7x + 11 \ \ [26]$ : il faut l'inverser.

On a $7x \equiv y - 11 \ \ [26]$ : on cherche donc $u$ tel que $7u \equiv 1 \ \ [26]$.

Autrement dit, $7u = 1 + 26v$ c'est-à-dire $7u - 26v = 1$.

On peut vérifier que $u = -11$ et $v = 3$ convient. Et à partir de là :

$-11 \times 7x \equiv -11(y - 11) \ \ [26]$

$-77x \equiv -11y + 121 \ \ [26]$

$x \equiv -11y + 17 \ \ [26]$ car $-77 \equiv 1 \ \ [26]$ et $121 \equiv 17 \ \ [26]$

Ainsi, $y = 17$ donne $x = -11 \times 17 + 17 = -170 \equiv 12 \ \ [26]$

De même, $y = 11$ donne $x = -11 \times 11 + 17 = -104 \equiv 0 \ \ [26]$

Et on finit donc par retrouver la séquence 12 / 0 / 19 / 7 / 18 laquelle redonne bien le mot MATHS.

Remarques : 1. Si $a = 1$, on obtient un codage correspondant au code de César.

2. La clé $a$ devant toujours être première avec 26, il y a donc 12 possibilités : 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23 et 25.

   Et avec 26 possibilités pour la clé $b$, cela fait $12 \times 26 = 312$ clés de chiffrement possibles : cryptage facile à casser donc, en testant ces 312 possibilités.

   ⇨ *Voir https://www.dcode.fr/chiffre-affine*

   On peut améliorer la fiabilité de cette méthode de cryptage en passant par les codes ASCII (minuscules, majuscules, chiffres…)

3. Bien d'autres techniques plus élaborées existent en cryptographie : le chiffrement de Hill (dont le principe est de coder non plus lettre à lettre mais par groupes de lettres) ou le code RSA (dont la clé de codage ne permet pas le décodage).

## II Théorème de Gauss

Théorème : Soient $a$, $b$ et $c$ des entiers strictement positifs.

Si $a|bc$ et $\text{PGCD}(a\,;b)=1$ alors $a|c$.

Autrement dit, si un entier naturel divise un produit de deux facteurs et qu'il est premier avec l'un d'eux, alors il divise l'autre.

Preuve : On sait que $a|bc$ donc $bc=ka$ avec $k\in\mathbb{Z}$.

Par ailleurs, $\text{PGCD}(a\,;b)=1$ donc d'après Bézout, $\exists(u\,;v)\in\mathbb{Z}^2, au+bv=1$.

En multipliant par $c$, on obtient $c(au+bv)=c$

$$acu+kav=c$$

$$a(cu+kv)=c$$ et donc $a|c$.

Méthode : Résolution d'une équation $ax+by=c$ avec $a$ et $b$ premiers entre eux

1. Déterminer une solution particulière $(x_0;y_0)$ de l'équation $ax+by=c$ :
   - ⇨ soit à l'aide de la calculatrice (en *vérifiant* que…)
   - ⇨ soit en commençant par trouver une solution de l'équation $ax+by=1$ par remontée de l'algorithme d'Euclide, puis en multipliant cette solution par $c$
2. Utiliser Gauss sachant que $ax+by=ax_0+by_0$ ➔ $a(x-x_0)=b(y-y_0)$

Ex : Déterminer les solutions de l'équation $89x+41y=5$.

On a déjà vu que $x=6$ et $y=-13$ est une solution de $89x+41y=1$.

Autrement dit, $89\times6+41\times(-13)=1$.

$$5(89\times6+41\times(-13))=5$$

$$89\times30+41\times(-65))=5$$

D'où $89x+41y=89\times30+41\times(-65))$

$$41y+41\times65=89\times30-89x$$

$$41(y+65)=89(30-x)$$

Or, 41 et 89 sont premiers entre eux donc $41|(30-x)$ d'après Gauss.

On a donc $30-x=41k$ où $k\in\mathbb{Z}$ c'est-à-dire $x=30-41k$.

D'où $41(y+65)=89\times41k$

$$y+65=89k$$

$$y=-65+89k$$

Les solutions de $89x+41y=5$ sont donc les couples $(30-41k\,;\,-65+89k)$ où $k\in\mathbb{Z}$.

Attention : On a vu que $41(y+65)=89(30-x)$. Le théorème de Gauss permet donc de dire que $41|(30-x)$ mais aussi que $89|(y+65)$.

Cela ne se traduit **pas** par $30-x=41k$ et $y+65=89k$ où $k\in\mathbb{Z}$.

On a en effet $30-x=41k$ où $k\in\mathbb{Z}$ et $y+65=89\boldsymbol{k'}$ où $k'\in\mathbb{Z}$.

Et il faut donc ensuite s'assurer que $k=k'$. C'est faisable :

$$41(y+65)=89(30-x)$$

$$41\times 89k'=89\times 41k$$

D'où $k'=k$.

Ex : Dans un repère orthonormé, on donne A(-3 ; 28) et B(24 ; 10). Déterminer les points de [AB] dont les coordonnées sont entières.

Commençons par chercher l'équation de la droite (AB).

$\overrightarrow{AB}\begin{pmatrix}27\\-18\end{pmatrix}$ dirige (AB) donc $\vec{u}\begin{pmatrix}3\\-2\end{pmatrix}$ est un vecteur directeur de (AB).

D'où (AB) : $-2x-3y+c=0$

Or, A ∈ (AB) par exemple : $-2\times(-3)-3\times 28+c=0$

$$6-84+c=0$$

$$c=78$$

Donc (AB) : $-2x-3y+78=0$, c'est-à-dire $2x+3y-78=0$

On a alors $2x+3(y-26)=0$

$$2x=3(26-y)$$

Puisque 2 et 3 sont premiers entre eux, alors $3|x$ d'après le théorème de Gauss.

On peut donc écrire $x=3k$ avec $k\in\mathbb{Z}$.

D'où $2\times 3k=3(26-y)$

$$2k=26-y$$

$$y=26-2k$$

Mais puisqu'on s'intéresse au *segment* [AB] alors $-3\leq x\leq 24$

$$-3\leq 3k\leq 24$$

$$-1\leq k\leq 8$$

Les solutions sont donc les 10 points de coordonnées $(3k\,;26-2k)$ avec $-1\leq k\leq 8$.

Corollaire : Si un entier naturel $n$ est divisible par deux entiers naturels $a$ et $b$ premiers entre eux, alors il est divisible par leur produit.

Généralisation : si un entier est divisible par plusieurs entiers premiers entre eux deux à deux, alors il est divisible par leur produit.

Preuve : On a $n = aq$ et $n = bq'$ donc $aq = bq'$.

Donc $b|aq$ ce qui implique que $b|q$ car $b$ est premier avec $a$. (théorème de Gauss)

On peut donc écrire $q = bp$.

D'où $n = aq = abp$ ce qui signifie bien que $ab|n$.

Ex : 2 295 est divisible par 5 car il se termine par un 5.

2 295 est divisible par 9 car la somme de ses chiffres est 18 et 18 est divisible par 9.

Or, 5 et 9 sont premiers entre eux donc 2 295 est divisible par $5 \times 9 = 45$.

C-ex : 12 est divisible par 2 et par 4 mais pas par 8 (2 et 4 ne sont pas premiers entre eux)

Ex : Soit $n$ un entier naturel non nul. Prouver que $A = n(n^4 - 1)$ est divisible par 30.

⇨ *Un tableau de congruences [30] est trop long. On va montrer que A est divisible par 2, 3 et 5 ; et donc qu'il est divisible par $2 \times 3 \times 5 = 30$ !*

On a $A = n(n^4 - 1)$

$= n(n^2 - 1)(n^2 + 1)$

$= n(n - 1)(n + 1)(n^2 + 1)$

⇨ $2|A$ car $n$ et $(n + 1)$ sont deux entiers consécutifs.

⇨ $3|A$ car $(n - 1)$, $n$ et $(n + 1)$ sont trois entiers consécutifs

Prouvons que $5|A$ en effectuant un tableau des congruences modulo 5 :

| $n$ | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| $n^2$ | 0 | 1 | 4 | 4 | 1 |
| $n^2 + 1$ | 1 | 2 | 0 | 0 | 2 |
| $n^2 - 1$ | 4 | 0 | 3 | 3 | 0 |
| A | 0 | 0 | 0 | 0 | 0 |

Ainsi, $5|A$.

Or, 2, 3 et 5 sont premiers entre eux deux à deux et $2 \times 3 \times 5 = 30$. Donc $30|A$.