Chapitre 13

Entiers relatifs et arithmétique

Sommaire

OBJECTIFS

Les objectifs sont particulièrement modestes, jugez plutôt :

- ▷ division euclidienne dans $\mathbf{Z}$, aglorithmes d'Euclide et de Bezout
- ▷ théorème de Bezout et application à la résolution des équations diophantiennes
- ▷ théorème de Gauss
- ▷ décomposition primaire des entiers

I Entiers relatifs

1 Z est structuré en anneau

L'ensemble $\mathbf{Z} = \{\ldots, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, \ldots\}$ des entiers relatifs est muni de deux lois : l'addition (notée $+$) et la multiplication (notée . ou sans symbole).

1.a Propriétés de l'addition

- **La loi $+$ est associative**, *i.e.* $\forall (a, b, c) \in \mathbf{Z} \times \mathbf{Z} \times \mathbf{Z}, (a + b) + c = a + (b + c)$,
- **la loi $+$ est commutative**, *i.e.* $\forall (a, b) \in \mathbf{Z} \times \mathbf{Z}, a + b = b + a$,
- **la loi $+$ possède un élément neutre**, c'est l'élément 0, $\forall a \in Z, a + 0 = a$,
- **tout entier $a \in \mathbf{Z}$ possède un élément symétrique** pour la loi $+$, c'est l'élément $-a : \forall a \in \mathbf{Z}, a+(-a) = 0$.

Vocabulaire : *on résume ces propriétés en disant que* $(\mathbf{Z}, +)$ *est un* ***groupe commutatif****.*

1.b Propriétés de la multiplication

Aux propriétés de l'addition viennent s'ajouter celles de la multiplication dans $\mathbf{Z}$, et celle combinant les deux lois :

- **La loi . est associative** : $\forall (a, b, c) \in \mathbf{Z} \times \mathbf{Z} \times \mathbf{Z}, (a.b).c = a.(b.c)$,
- **la loi . est commutative** : $\forall (a, b) \in \mathbf{Z} \times \mathbf{Z}, a.b = b.a$,
- **la loi . est distributive par rapport à l'addition :** $\forall (a, b, c) \in \mathbf{Z} \times \mathbf{Z} \times \mathbf{Z}, (a + b).c = a.c + b.c$,
- **la loi . possède un élément neutre**, c'est l'élément $1 : \forall a \in \mathbf{Z}, 1.a = a$.
- **Z est intègre** $\forall (a, b) \in \mathbf{Z} \times \mathbf{Z},\ a.b = 0 \Rightarrow (a = 0)$ *ou* $(b = 0)$.

Vocabulaire : *l'ensemble des propriétés décrites ci-dessus font de* $(\mathbf{Z}, +, .)$ *un* ***anneau commutatif****.*

Remarque : on peut définir aussi l'**inverse** pour la loi . : l'inverse de $a \in \mathbf{Z}$ est l'élément $b \in \mathbf{Z}$, s'il existe, tel que $a.b = 1$. Les seuls éléments de $\mathbf{Z}$ qui possèdent un inverse pour la multiplication sont $\mathbf{Z}^\times = \{-1, 1\}$.

2 Multiples et diviseurs

2.a Relation de divisibilité

Définition : *Soit a et b deux entiers relatifs. On dit que a est un* ***multiple*** *de b ou que b est un* ***diviseur*** *de a, s'il existe $q \in \mathbf{Z}$ tel que $a = bq$. On note cette relation $b \mid a$.*

Exemples :

- $2 \mid 6$ et $2 \nmid 3$.
- 0 est multiple de tous les entiers relatifs, mais ne divise que lui-même.
- 1 divise tout entier, mais ce n'est un multiple que de 1 et -1.

Exercice : Montrez que pour tout entier $n \in \mathbf{N}$, 11 divise $3^{n+3} - 4^{4n+2}$.

Proposition 13.1.— Soit $(a,b) \in \mathbf{Z}^2$. Alors b divise a *si et seulement si* $|b|$ divise $|a|$.

Conséquence : le signe des entiers n'influe aucunement les questions de divisibilité, ce qui permet de se ramener systématiquement au cadre d'entiers naturels.

Démonstration ▽
Raisonnons par équivalences.

$$b \mid a \iff \exists q \in \mathbf{Z}, a = bq \iff \exists q \in \mathbf{Z}, |a| = |b|q \iff |b| \mid |a|.$$

▲

Proposition 13.2.— Soit $(a,b,c,d) \in \mathbf{Z}^4$,

- si $a \mid b$ et $b \mid c$, alors $a \mid c$
- si $a \mid b$ et $a \mid c$, alors $a \mid b+c$
- si $a \mid b$ et $b \neq 0$, alors $|a| \leq |b|$.
- si $a \mid b$ et $c \mid d$, alors $ac \mid bd$
- si $a \mid b$, alors pour tout $p \in \mathbf{N}$, $a^p \mid b^p$
- si $a \mid b$ et $b \mid a$, alors $|a| = |b|$.

Démonstration ▽

- si $a \mid b$ et $b \mid c$, alors il existe $(k,\ell) \in \mathbf{Z}^2$ tel que $b = ak$ et $c = b\ell$. Par suite $c = k\ell a$.
- si $a \mid b$ et $a \mid c$, alors, il existe $(k,\ell) \in \mathbf{Z}^2$ tel que $b = ak$ et $c = a\ell$. Par suite $b + c = ka + \ell a = a(k+\ell)$.
- si $a \mid b$ et $b \neq 0$, alors, il existe $k \in \mathbf{Z}^\star$ tel que $b = ak$. D'où $|b| = |a| \times |k|$. Comme $k \neq 0$, $|k| \geq 1$, par suite, $|b| \geq |a|$.
- si $a \mid b$ et $c \mid d$, alors il existe $(k,\ell) \in \mathbf{Z}^2$ tel que $b = ak$ et $d = c\ell$. Par suite $bd = (k\ell)ac$.
- par récurrence sur p à partir de la propriété précédente.
- si $b = 0$, alors $a = 0$. Si $b \neq 0$, alors $a \neq 0$ et par conséquent $|a| \leq |b|$ et $|b| \leq |a|$. ▲

Exercice : Soit $a \in \mathbf{Z}$ et $d \in \mathbf{N}$. Montrez que si $d \mid a$ et $d \mid a^2 + a + 1$, alors $d = 1$.

2.b Multiples et diviseurs d'un entier

Définition : *Soit $a \in \mathbf{Z}$, on définit*

- *l'ensemble des multiples de a :* $\mathcal{M}(a) = \{b \in \mathbf{Z} \mid \exists q \in \mathbf{Z};\ b = q.a\} = \{a.q;\ q \in \mathbf{Z}\}$.
- *l'ensemble des diviseurs de a :* $\mathcal{D}(a) = \{b \in \mathbf{Z} \mid \exists q \in \mathbf{Z},\ a = b.q\}$.

Notation : *On note aussi* $\mathcal{M}(a) = a\mathbf{Z}$.

Remarque : $\mathcal{M}(a)$ et $\mathcal{D}(a)$ sont symétriques par rapport à 0.

Exemples :

1. $\mathcal{D}(6) = \{-6,-3,-2,-1,1,2,3,6\}$, $\mathcal{D}(1) = \{-1,1\}$, $\mathcal{D}(0) = \mathbf{Z}$
2. L'ensemble $2\mathbf{Z}$ des multiples de 2 est l'ensemble des nombres entiers relatifs pairs.
3. $\mathcal{M}(0) = \{0\}$

La relation de divisibilité peut se traduire à l'aide d'inclusion ensemblistes :

Proposition 13.3.— Soit $(a,b) \in \mathbf{Z}^2$. Les assertions suivantes sont équivalentes :

⇕
- $a \mid b$ — *a divise b*
- $\mathcal{D}(a) \subset \mathcal{D}(b)$ — *tout diviseur de a divise b*
- $\mathcal{M}(b) \subset \mathcal{M}(a)$ — *tout multiple de b est multiple de a*

Exercice : Résolvez les équations suivantes :

1. Pour quels entiers $x \in \mathbf{Z}$ a-t-on $x - 1 \mid x + 3$?
2. Pour quels couples d'entiers $(x,y) \in \mathbf{Z}^2$ a-t-on $xy = 2x + 3y$?

Solution ▽

1. *Soit $x \in \mathbf{Z}$, on a les équivalences suivantes :*

$$\begin{aligned} x-1 \mid x+3 &\iff \exists k \in \mathbf{Z},\ x+3 = k(x-1) \\ &\iff \exists k \in \mathbf{Z},\ (x-1)+4 = k(x-1) \\ &\iff \exists \ell \in \mathbf{Z},\ 4 = \ell(x-1) \\ &\iff \begin{cases} x' = x-1 \\ x' \mid 4 \end{cases} \end{aligned}$$

Ainsi

x'	-4	-2	-1	2	4
$x'+1$	-3	-1	0	3	5

Par conséquent l'ensemble des solutions est $\mathcal{S} = \{-3, -1, 0, 3, 5\}$.

2. *Soit $(x, y) \in \mathbf{Z}^2$. On a*

$$\begin{aligned} xy = 2x + 3y &\iff xy - 2x - 3y = 0 \\ &\iff (x-3)(y-2) = 6 \\ &\iff \begin{cases} x' = x-3 \\ y' = y-2 \\ x' \times y' = 6 \end{cases} \end{aligned}$$

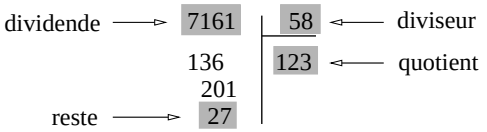
Ainsi

x'	-6	-3	-2	-1	1	2	3	6
$x'+3$	-3	0	1	2	4	5	6	9
$y'+2$	1	0	-1	-4	8	5	4	3
y'	-1	-2	-3	-6	6	3	2	1

Par conséquent l'ensemble solution est $\big\{(-3,1); (0,0); (1,-1); (2;-4); (4,8); (5,5); (6,4); (9,3)\big\}$. ▲

3 Division euclidienne dans Z

Dans $\mathbf{Z}$, les seuls éléments inversibles pour la multiplication sont ± 1. On utilise la division euclidienne, telle qu'elle a été introduite au collège.



Plus théoriquement,

Théorème 13.4.— Division euclidienne dans Z
Pour tout couple $(a, b) \in \mathbf{Z} \times \mathbf{N}^\star$ d'entiers, il **existe** un couple $(q, r) \in \mathbf{Z}^2$, **unique** tel que

- $a = bq + r$
- $0 \leq r < b$

Vocabulaire :

- *q est appelé le **quotient** de la division euclidienne de a par b.*
- *r est appelé le **reste** de la division euclidienne de a par b.*

Warning : les deux conditions sont nécessaires pour pouvoir parler de division euclidienne.

Exemples :

- $a = 53$, $b = 4$: $53 = 4 \times 13 + 1$ et $0 \leq 1 < 4$ donc $(q, r) = (13, 1)$.
- $a = -52$, $b = 7$: $-52 = 7 \times (-8) + 4$ et $0 \leq 4 < 7$, donc $(q, r) = (-8, 4)$.

- $a = 267$, $b = 37$: $267 = 18 \times 37 - 399$, mais $(q, r) \neq (18, -399)$!

Démonstration ▽
Il s'agit d'un résultat d'existence et d'unicité. La preuve sera en deux étapes :

■**Unicité :** commençons par prouver l'unicité du couple quotient, reste.
Soit donc $((q_1, r_1), (q_2, r_2)) \in (\mathbf{Z} \times \mathbf{N}^\star)^2$ tel que

$$\left\| \begin{array}{rcll} a & = & bq_1 + r_1 & 0 \leq r_1 \leq b-1 \\ a & = & bq_2 + r_2 & 0 \leq r_2 \leq b-1 \end{array} \right.$$

On en déduit que $b(q_2 - q_1) = r_1 - r_2$ d'où

$$|b||q_1 - q_2| = |r_1 - r_2|$$

Comme d'autre part $|r_1 - r_2| < |b|$ ceci entraîne successivement que $|q_1 - q_2| = 0$ puis $q_1 = q_2$ et finalement $r_1 = r_2$.

■**Existence :**

- Montrons tout d'abord l'existence de (q, r) dans **le cas où** $(a, b) \in \mathbf{N} \times \mathbf{N}^\star$:
  Soit donc $(a, b) \in \mathbf{N} \times \mathbf{N}^\star$, notons $\mathbb{B}_a = \{m \in \mathcal{M}(b) \mid \ m \leq a\}$ l'ensemble des multiples de b inférieurs ou égaux à a. Par construction,
  - $\mathbb{B}_a$ est majoré par a.
  - $\mathbb{B}_a$ est non vide car $0 = 0.b \in \mathbb{B}_a$.

  D'après la propriété fondamentale ($\mathbf{N}_2$) de $\mathbf{N}$, $\mathbb{B}_a$ possède un plus grand élément. Notons-le $m = b.q$. Soit alors $r = a - m = a - bq$ de sorte que
  - $a = m + r = bq + r$
  - $r \geq 0$ car $m \leq a$

  D'autre part, $M = m + b = bq + b$ est clairement un multiple de b, *strictement* supérieur à m. Comme m est le plus grand élément de $\mathbb{B}_a$, M ne saurait appartenir à $\mathbb{B}_a$. Par conséquent, $M > a$. Ainsi, $bq + b > bq + r$, d'où je tire $0 \leq r < b$. Finalement, le couple (q, r) convient.
- Dans **le cas où** $(a, b) \in \mathbf{Z}^- \times \mathbf{N}^\star$, appliquons le résultat ci-dessus à $(|a|, b) \in \mathbf{N} \times \mathbf{N}^\star$: il existe donc un couple $(\tilde{q}, \tilde{r}) \in \mathbf{N} \times [\![0, b-1]\!]$ tel que
  $$-a = b\tilde{q} + \tilde{r}$$
  - Si $\tilde{r} = 0$, posons $q = -\tilde{q}$. Le couple $(q, 0)$ convient.
  - Si $\tilde{r} > 0$, alors
  $$\begin{array}{rcl} a & = & b(-\tilde{q}) + (-\tilde{r}) \\ & = & b(-\tilde{q}) - b + b + (-\tilde{r}) \\ & = & b(-\tilde{q} - 1) + (b - \tilde{r}). \end{array}$$
  Posons finalement $q = -\tilde{q} - 1$ et $r = b - \tilde{r}b$. Nous obtenons donc $a = b.q + r$, avec $q \in \mathbf{Z}$ et $r \in [\![1, b-1]\!]$. Le couple (q, r) convient.
- Pour tout couple $(a, b) \in \mathbf{Z} \times \mathbf{N}^\star$, nous avons donc construit un couple $(q, r) \in \mathbf{Z} \times [\![0, b-1]\!]$, tel que $a = b.q + r$.

▲

Exercice : Soit $(a, b, n) \in \mathbf{N}^\star \times \mathbf{N}^\star \times \mathbf{N}$. On note q le quotient de la division euclidienne de $a-1$ par b. Déterminez le quotient de la division euclidienne de $ab^n - 1$ par b^{n+1}.

Proposition 13.5.— Soit $(a, b) \in \mathbf{Z} \times \mathbf{N}^\star$.

b divise a *si et seulement si* le reste de la division euclidienne de a par b est nul.

Démonstration ▽

- si le reste est nul, la division euclidienne de a par b s'écrit $a = bq$, où $q \in \mathbf{Z}$. Par suite b divise a.
- si b divise a, il existe $q \in \mathbf{Z}$ tel que $a = b \times q = b \times q + 0$. Comme $0 \leq 0 < b$, il s'agit de la division euclidienne de a par b. En particulier, le reste est nul. ▲

II PGCD et PPCM de deux entiers relatifs

1 PGCD de deux entiers relatifs

1.a Diviseurs communs à deux entiers

Définition : *Soit $(a,b) \in \mathbf{Z}^2$ un couple d'entiers relatifs et $d \in \mathbf{Z}$.*
On dit que $d \in \mathbf{Z}$ est un ***diviseur commun*** *à a et b si $d \mid a$ et $d \mid b$.*

Notation : *On note $\mathcal{D}(a,b)$ l'ensemble des diviseurs communs à a et b. On a $\mathcal{D}(a,b) = \mathcal{D}(a) \cap \mathcal{D}(b)$.*

Exemple : $\mathcal{D}(24,18) = \{-6,-3,-2,-1,1,2,3,6\} = \mathcal{D}(6)$.

Lemme 13.6.— Soit $(a,b) \in \mathbf{Z}^2$ un couple d'entiers relatifs, tel que $(a,b) \neq (0,0)$.

L'ensemble des éléments de $\mathbf{N}^\star$, diviseurs communs à a et b est non vide et majoré. Il admet donc un plus grand élément.

Démonstration ▽

- $1 \in \mathcal{D}(a,b)$ car 1 divise tout entier. L'ensemble des éléments de $\mathbf{N}^\star$ divisant a et b est non vide.
- Supposons sans perte de généralité que $a \neq 0$. Tout diviseur de a est majoré par $|a|$. *A fortiori*, l'ensemble des éléments de $\mathbf{N}^\star$ divisant a et b l'est aussi.

Ainsi, l'ensemble des éléments de $\mathbf{N}^\star$, diviseurs communs à a et b est non vide et majoré. Il suffit alors d'invoquer la propriété ($\mathbf{N}_2$) des entiers naturels pour conclure à l'existence d'un plus grand élément. ▲

1.b Plus grand diviseur commun de deux entiers

Proposition-Définition 13.7.— Soit $(a,b) \in \mathbf{Z}^2$ un couple d'entiers relatifs, tel que $(a,b) \neq (0,0)$. Le plus grand élément de $\mathcal{D}(a,b)$ est appelé **plus grand diviseur commun** à a et b. On note $\mathrm{PGCD}(a,b)$ ou $a \wedge b$ cet entier naturel :

$$\boxed{\mathrm{PGCD}(a,b) = a \wedge b = \max\{d \in \mathbf{N}^\star \mid d \mid a \text{ et } d \mid b\}}$$

Notation : *on convient que* $\mathrm{PGCD}(0,0) = 0 \wedge 0 = 0$.

Exemple : $a \wedge a = |a|$, $a \wedge 1 = 1$, $a \wedge 0 = |a|$.

Remarque : le PGCD de deux entiers ne dépend pas du signe de ces derniers. En effet,

$$\forall (a,b) \in \mathbf{Z}^2, \quad a \wedge b = |a| \wedge |b|$$

1.c Algorithme d'Euclide

Pour calculer le PGCD de deux entiers, nous procédons de proche en proche, en effectuant des divisions euclidiennes successives :

Proposition 13.8.— Lemme d'Euclide —. Soit $(a,b) \in \mathbf{Z} \times \mathbf{N}^\star$. Notons r le reste de la division euclidienne de a par b. Alors

$$\boxed{a \wedge b = b \wedge r}$$

Démonstration ▽
La division euclidienne de a par b s'écrit $a = bq + r$ avec $0 \leq r < b$. Montrons par double-inclusion que $\mathcal{D}(a,b) = \mathcal{D}(b,r)$. Un moyen radical de montrer que a et b d'une part, b et r d'autre part ont le même plus grand diviseur commun !

- $\mathcal{D}(a,b) \subset \mathcal{D}(b,r)$: soit $d \in \mathcal{D}(a,b)$ un diviseur commun à a et b. *A fortiori* d divise a et bq. Par conséquent, d divise b et $r = a - bq$.
- $\mathcal{D}(a,b) \subset \mathcal{D}(b,r)$: soit $d \in \mathcal{D}(b,r)$ un diviseur commun de b et r. En ce cas, d divise aussi $bq + r$. Ce qui entraîne que d divise b et a. ▲

Remarques :

1. si $r = 0$, alors $a \wedge b = b \wedge 0 = |b|$.

2. si $b \mid a$, alors $a \wedge b = |b|$.

Mise en œuvre

On souhaite calculer $d = a \wedge b$. Notons $a_0 = \max\{|a|, |b|\}$ et $a_1 = \min\{|a|, |b|\}$, de sorte que $d = a_0 \wedge a_1$.

- **Étape 1** deux cas se présentent :
  - si $a_1 = 0$, alors $d = a_0 \wedge a_1 = a_0$.
  - si $a_1 \neq 0$, effectuons la division euclidienne de a_0 par a_1.

$$a_0 = q_1 a_1 + a_2, \text{ où } 0 \leq a_2 < a_1,$$

  D'après la proposition précédente, $d = a_1 \wedge a_2$. On passe à l'

- **Étape 2** deux cas se présentent :
  - si $a_2 = 0$, alors $d = a_0 \wedge a_1 = a_1 \wedge a_2 = a_1$.
  - si $a_2 \neq 0$, effectuons la division euclidienne de a_1 par a_2.

$$a_1 = q_2 a_2 + a_3, \text{ où } 0 \leq a_3 < a_2$$

  D'après la proposition précédente, $d = a_2 \wedge a_3$.

- **Étape 3** Ainsi de suite ...

Comme $a_0, a_1, a_2, a_3 \ldots$ sont des entiers naturels et $a_0 \geq a_1 > a_2 > a_3 > \cdots$, il existe un entier $m \in \mathbf{N}$ tel que a_{m+1} soit nul. Si tel est le cas,

$$d = a_m \wedge a_{m+1} = a_m \wedge 0 = a_m$$

Résumons :

Proposition 13.9.— Soit $(a, b) \in \mathbf{Z}^2$.

Le PGCD de a et b est le dernier reste non nul dans l'algorithme d'Euclide.

Exemple : Calculons le PGCD de 162 et 207.

$$\begin{aligned} 207 &= 1 \times 162 + 45 \\ 162 &= 3 \times 45 + 27 \\ 45 &= 1 \times 27 + 18 \\ 27 &= 1 \times 18 + \boxed{9} \\ 18 &= 2 \times 9 + 0 \end{aligned}$$

D'où $207 \wedge 162 = 9$.

Exercice : Calculez les PGCD de a et b lorsque

1. $a = 24$, $b = 9$

2. $a = 15$ et $b = 28$

3. $a = -60$ et $b = -80$.

1.d Égalité de Bezout

Théorème 13.10.— Soit $(a,b) \in \mathbf{Z}^2$. Il existe $(u,v) \in \mathbf{Z}^2$ tel que

$$\boxed{au + bv = a \wedge b}$$

Vocabulaire : *une telle égalité est appelée égalité de Bezout.*

Remarques :

1. Les coefficients u et v, appelés **coefficients de Bezout**, ne sont pas uniques. Par exemple, $6 \wedge 9 = 3$ et $3 = -1 \times \mathbf{6} + 1 \times \mathbf{9} = 8 \times \mathbf{6} - 5 \times \mathbf{9}$
2. Si $d = a \wedge b$, alors il existe $(u,v) \in \mathbf{Z}^2$ tel que $au + bv = d$. La réciproque est fausse. Par exemple, $3 \times 6 - 1 \times 10 = 8$, mais le PGCD de 6 et 10 est 2, et non pas 8.

Démonstration ▽
Effectuons l'algorithme d'Euclide. Nous obtenons une liste $a_0, a_1, \ldots, a_m, a_{m+1}$ d'entiers telle que

$$\left\| \begin{array}{l} a_0 \geq a_1 > a_2 \cdots > a_m > a_{m+1}, \text{ avec } a_{m+1} = 0, a_m = a \wedge b, \text{ et} \\ \forall k \in [\![0, m-1]\!],\ a_k = q_{k+1} a_{k+1} + a_{k+2} \end{array} \right.$$

Ainsi

$$\left\{ \begin{array}{ccccccccc} a_0 & -q_1 a_1 & & & & & & & = a_2 \\ & a_1 & -q_2 a_2 & & & & & & = a_3 \\ & & \ddots & \ddots & & & & & \vdots \\ & & & a_{m-3} & -q_{m-2} a_{m-2} & & & & = a_{m-1} \\ & & & & & a_{m-2} & -q_{m-1} a_{m-1} & & = a_m \end{array} \right.$$

Par *remontée*, on en déduit que $a \wedge b$ s'écrit comme combinaison linéaire de a et b. En effet,

- D'après la dernière équation, nous déduisons que $a_m = a \wedge b$ est combinaison linéaire de a_{m-2} et a_{m-1},
- Or d'après l'avant-dernière équation, a_{m-1} est lui-même combinaison linéaire de a_{m-3} et a_{m-2}, on en déduit que $a \wedge b$ est combinaison linéaire de a_{m-3} et a_{m-2},
- ainsi de suite ...
- à la fin, $a \wedge b$ s'exprime comme combinaison linéaire de a_0 et a_1. Comme a_0 et a_1 sont égaux à $\pm a$, et $\pm b$, il s'ensuit que $a \wedge b$ s'écrit comme combinaison linéaire de a et b.

▲

En pratique : la démonstration présentée ci-dessus est constructive : pour établir une égalité de Bezout pour deux entiers a et b, vous *remontez* l'algorithme d'Euclide.

Exercice : Déterminez le PGCD d de a et b et obtenez une égalité de Bezout lorsque

1. $a = 150$ et $b = 54$
2. $a = -11$ et $b = 25$.

Solution ▽

L'algorithme d'Euclide donne tout d'abord

$$\begin{array}{rcl} 150 &=& 2 \times 54 + 42 \\ 54 &=& 1 \times 42 + 12 \\ 42 &=& 3 \times 12 + \boxed{6} \\ 12 &=& 2 \times 6 + 0 \end{array}$$

Ainsi $150 \wedge 54 = 6$.

On procède ensuite par remontée :

$$\begin{array}{rcl} 6 &=& 42 - 3 \times 12 \\ &=& 42 - 3 \times (54 - 42) = 4 \times 42 - 3 \times 54 \\ &=& 4 \times (150 - 2 \times 54) - 3 \times 54 \end{array}$$

Soit $4 \times 150 - 11 \times 54 = 1$. ▲

1.e Caractérisations du PGCD

Le théorème suivant donne deux caractérisations du PGCD de deux entiers :

Théorème 13.11.— Caractérisations du PGCD —. Soit $(a,b)\in\mathbf{Z}^2$, on note $a.\mathbf{Z}+b.\mathbf{Z}=\{a.k+b.\ell,;\ (k,\ell)\in\mathbf{Z}^2\}$ l'ensemble des combinaisons linéaires à coefficients entiers de a et b.
Pour tout entier **naturel** $d\in\mathbf{N}$, les assertions suivantes sont équivalentes :

$$\left\Updownarrow\begin{array}{rl} i) & d=a\wedge b\\ ii) & a\mathbf{Z}+b\mathbf{Z}=d\mathbf{Z}\\ iii) & \mathcal{D}(a,b)=\mathcal{D}(d)\end{array}\right.$$

Commentaires :

- La définition de P GRAND CD fait appel à la structure d'ensemble ordonné de $\mathbf{Z}$.
- Le deuxième point est une **caractérisation algébrique** du PGCD. Il est fondamental pour la structure algébrique de $\mathbf{Z}$, et pour la résolution des équations algébriques du type $ax+by=c$, voir le corollaire plus bas.
- Le troisième point est une **caractérisation arithmétique** du PGCD. Il montre que tout diviseur commun à a et b divise $a\wedge b$.

Démonstration ▽
Si $d=0$, on a bien $a\wedge b=0\iff a=0$ et $b=0\iff a\mathbf{Z}+b\mathbf{Z}=\{0\}\iff\mathcal{D}(a,b)=\mathbf{Z}$. Supposons désormais que $d\in\mathbf{N}^\star$.

$i\Rightarrow ii$ soit $d=a\wedge b$. On montre que $a\mathbf{Z}+b\mathbf{Z}=d\mathbf{Z}$ par double inclusion.
Comme d divise a et b alors $a\in d\mathbf{Z}$ et $b\in d\mathbf{Z}$. Par conséquent $a\mathbf{Z}+b\mathbf{Z}\subset d\mathbf{Z}$. Réciproquement l'égalité de Bezout montre qu'il existe $(u,v)\in\mathbf{Z}^2$ tels que $d=au+bv$. Ainsi, $d\in a\mathbf{Z}+b\mathbf{Z}$. Par suite, $d\mathbf{Z}\subset a\mathbf{Z}+b\mathbf{Z}$.

$ii\Rightarrow iii$ supposons que $a\mathbf{Z}+b\mathbf{Z}=d\mathbf{Z}$ et montrons que $\mathcal{D}(a,b)=\mathcal{D}(d)$.
Tout d'abord, $a,b\in a\mathbf{Z}+b\mathbf{Z}=d\mathbf{Z}$. Donc $d\in\mathcal{D}(a)\cap\mathcal{D}(b)=\mathcal{D}(a,b)$. Par conséquent, $\mathcal{D}(d)\subset\mathcal{D}(a,b)$. Réciproquement, soit $q\in\mathcal{D}(a,b)$, alors il existe $(k,\ell)\in\mathbf{Z}^2$, tel que $a=qk$ et $b=q\ell$. Comme par hypothèse $d\mathbf{Z}=a\mathbf{Z}+b\mathbf{Z}$, il existe $(u,v)\in\mathbf{Z}^2$ tel que $d=au+bv$. Par suite d s'écrit $d=u(kq)+v(\ell q)=(uk+v\ell)q$. En particulier, q divise d, ie. $q\in\mathcal{D}(d)$.

$iii\Rightarrow i$ supposons que $\mathcal{D}(a,b)=\mathcal{D}(d)$. En particulier, ces ensembles ont le même plus grand élément, à savoir $d=a\wedge b$.▲

Corollaire 13.12.— Condition de compatibilité des équations diophantiennes —. Soit $(a,b,c)\in\mathbf{Z}^3$. On considère l'équation diophantienne

$$ax+by=c \qquad (E)$$

(E) admet (au moins) une solution *si et seulement si* $a\wedge b$ divise c.

Démonstration ▽
D'après la **caractérisation algébrique du PGCD** (E) *est compatible* $\iff c\in a\mathbf{Z}+b\mathbf{Z}\iff c\in(a\wedge b)\mathbf{Z}\iff a\wedge b\mid c$.▲

Corollaire 13.13.— Homogénéité du PGCD —. Soit $(a,b)\in\mathbf{Z}^2$ et $k\in\mathbf{Z}$, alors

$$\boxed{\mathrm{PGCD}(ka,kb)=|k|\ \mathrm{PGCD}(a,b)}$$

Exemple : $\mathrm{PGCD}(80,-60)=20\mathrm{PGCD}(4,-3)=20$.

Démonstration ▽
Pour calculer le PGCD de ka et kb, j'utilise la **caractérisation algébrique du PGCD**. Soit $m\in\mathbf{Z}$. Alors

$$\big((ka)\wedge(kb)\big)\mathbf{Z}=ka\mathbf{Z}+kb\mathbf{Z}=k\big(a\mathbf{Z}+b\mathbf{Z}\big)=|k|(a\wedge b)\mathbf{Z}$$

D'après la caractérisation algébrique du PGCD, c'est dire que $\mathrm{PGCD}(ka,kb)=|k|\mathrm{PGCD}(a,b)$. ▲

2 PPCM de deux entiers

2.a Multiples communs à deux entiers

Définition : *Soit* $(a,b) \in \mathbf{Z}^\star \times \mathbf{Z}^\star$ *un couple d'entiers relatifs non nuls et* $m \in \mathbf{Z}$.
On dit que $m \in \mathbf{Z}$ *est un* ***multiple commun*** *à* a *et* b *si* $a \mid$ *et* $b \mid m$.

Notation : *On note* $\mathcal{M}(a,b)$ *l'ensemble des multiples communs à* a *et* b *:* $\mathcal{M}(a,b) = \mathcal{M}(a) \cap \mathcal{M}(b) = a\mathbf{Z} \cap b\mathbf{Z}$.

Exemple : 0, ab sont des multiples communs à a et b.

Lemme 13.14.— Soit $(a,b) \in (\mathbf{Z}^\star)^2$ un couple d'entiers relatifs, non nuls. L'ensemble $\mathcal{M}^+(a,b)$ des éléments de $\mathbf{N}^\star$ multiples communs à a et b est une partie non vide de $\mathbf{N}^\star$. Il admet donc un plus petit élément.

Démonstration ▽
Comme a et b sont non nuls, $|ab|$ est élément de $\mathcal{M}^+(a,b)$. En particulier, $\mathcal{M}^+(a,b)$ est non vide de $\mathbf{N}^\star$. D'après la propriété $(\mathbf{N}_1)$ des entiers naturels $\mathcal{M}^+(a,b)$ possède un plus petit élément. ▲

2.b Plus petit multiple commun de deux entiers

Proposition-Définition 13.15.— Soit $(a,b) \in \mathbf{Z}^\star \times \mathbf{Z}^\star$ un couple d'entiers relatifs non nuls. Le plus petit entier strictement positif élément de $\mathcal{M}(a,b)$ est appelé **plus petit multiple commun** à a et b. On note $\mathrm{PPCM}(a,b)$ ou $a \vee b$ cet entier naturel :

$$\mathrm{PPCM}(a,b) = a \vee b = \min\{m \in \mathbf{N}^\star \ \mid \ a \mid m \text{ et } b \mid m\}$$

Warning : le PPCM de deux entiers est en fait le plus petit multiple commun strictement positif de deux entiers.

Notation : *on convient que si* $a = 0$ *ou* $b = 0$, *alors* $\mathrm{PPCM}(a,b) = 0$.

Exemples :

- pour tout entier $a \in \mathbf{Z}$, $a \vee a = |a|$, $a \vee 1 = |a|$.
- $\mathrm{PPCM}(12,18) = 36$.

Remarque : le PPCM de deux entiers ne dépend pas du signe de ces derniers : $\forall (a,b) \in \mathbf{Z}^2, \quad a \vee b = |a| \vee |b|$.

2.c Caractérisations du PPCM

Théorème 13.16.— Caractérisations du PPCM —. Soit $(a,b) \in \mathbf{Z}^2$.
Pour tout entier **naturel** $m \in \mathbf{N}$, les assertions suivantes sont équivalentes :

$$\Updownarrow \begin{array}{ll} i) & m = a \vee b \\ ii) & a\mathbf{Z} \cap b\mathbf{Z} = m\mathbf{Z} \\ iii) & \mathcal{M}(a,b) = \mathcal{M}(m) \end{array}$$

Commentaires : les multiples communs à a et b, sont les multiples de $a \vee b$, $a\mathbf{Z} \cap b\mathbf{Z} = (a \vee b)\mathbf{Z}$.

Démonstration ▽
lorsque m est nul, on a $a \vee b = 0 \iff a = 0$ ou $b = 0 \iff a\mathbf{Z} \cap b\mathbf{Z} = \{0\}$. Supposons désormais que m est non nul.

$i \Rightarrow ii$ supposons que $m = a \vee b$, montrons que $a\mathbf{Z} \cap b\mathbf{Z} = m\mathbf{Z}$ par double-inclusion :
Par définition, m est un multiple commun de a et b. Par conséquent, tout multiple de m est un multiple de a et b, c'est-à-dire que $m\mathbf{Z} \subset a\mathbf{Z} \cap b\mathbf{Z}$.
Réciproquement, si $\nu \in a\mathbf{Z} \cap b\mathbf{Z}$ est un multiple commun à a et b, montrons que ν est un multiple de m. Effectuons la division euclidienne de ν par $m \in \mathbf{N}^\star$ $\nu = qm + r$, où $0 \leq r < m$. L'entier naturel r s'écrit comme la différence de deux multiples communs à a et b : $r = \nu - qm$. Par conséquent, r est un multiple commun à a et b. Comme $0 \leq r < m$, r est donc strictement inférieur au plus petit multiple commun strictement positif de a et b. Par conséquent, $r = 0$. Autrement dit ν est un multiple de m, *i.e.* $\nu \in m\mathbf{Z}$.

$ii \Rightarrow iii$ évident

iii $\Rightarrow$ *i* Supposons que $\mathcal{M}(a,b) = \mathcal{M}(m)$. En particulier ces deux ensembles ont le même plus petit élément strictement postif : $m = \text{PPCM}(a,b)$. ▲

Corollaire 13.17.— Homogénéité du PPCM —. Soit $(a,b) \in \mathbf{Z}^2$ et $k \in \mathbf{Z}$, alors

$$\boxed{\text{PPCM}(ka,kb) = |k|\ \text{PPCM}(a,b)}$$

Démonstration ▽
Elle découle grâce à la caractérisation algébrique de l'égalité ensembliste $ka\mathbf{Z} \cap kb\mathbf{Z} = k(a \vee b)\mathbf{Z} = |k|(a \vee b)\mathbf{Z}$. ▲

III Nombres premiers entre eux

1 Définition, exemples

Définition : *Soit $(a,b) \in \mathbf{Z}^2$. On dit que deux* ***entiers*** *a* ***et*** *b* ***sont premiers entre eux*** *s'ils n'ont pas d'autres diviseurs communs que -1 et 1 c'est-à-dire si $\mathcal{D}(a,b) = \{+1,-1\}$.*

Exemple : 22 et 35 sont premiers entre eux, 22 et 56 ne sont pas premiers entre eux.

Proposition 13.18.— Soit $(a,b) \in \mathbf{Z}^2$.

$$\boxed{a \text{ et } b \text{ sont premiers entre eux } \textit{si et seulement si } a \wedge b = 1.}$$

Démonstration ▽
a et b sont premiers entre eux *ssi* $\mathcal{D}(a,b) = \{-1,1\}$ *ssi* $\mathcal{D}(a \wedge b) = \{-1,1\}$ *ssi* $\mathcal{D}(a \wedge b) = \mathcal{D}(1)$. ▲

2 Théorème de Bezout

Il s'agit du résultat principal concernant les nombres premiers entre eux, qui donne une caractérisation des nombres premiers entre eux.
Étant donnés deux entiers a et b, nous avons déjà montré l'implication

$$d = a \wedge b \Rightarrow \exists (u,v) \in \mathbf{Z}^2,\ au + bv = a \wedge b$$

En revanche, la réciproque est fausse en général. C'est néanmoins le cas, lorsque $d = 1$:

Théorème 13.19.— Théorème de Bezout —. Soit $(a,b) \in \mathbf{Z}^2$.

$$\boxed{a \wedge b = 1 \iff \exists (u,v) \in \mathbf{Z}^2,\ au + bv = 1}$$

Démonstration ▽
Si a et b sont premiers entre eux, il existe des coefficients de Bezout $(u,v) \in \mathbf{Z}^2$ tels que $a \wedge b = au + bv$.
Réciproquement, s'il existe $(u,v) \in \mathbf{Z}^2$ tels que $au + bv = 1$. Il en résulte par double-inclusion que $a\mathbf{Z} + b\mathbf{Z} = \mathbf{Z}$. D'après la caractérisation algébrique du PGCD, il en découle finalement que $a \wedge b = 1$. ▲

Exemple : Soit $n \in \mathbf{Z}$. n et $n+1$ sont premiers entre eux, car $1 = (n+1) - n$.

Exercice : Soit $(a,b,c) \in \mathbf{Z}^3$. On suppose que c divise a et que a et b sont premiers entre eux. Montrez que c et b sont premiers entre eux.

Warning : rappelons qu'il n'y a pas unicité du couple de coefficients de Bezout. Par exemple $2 \times 2 - 1 \times 3 = 5 \times 2 - 3 \times 3 = 1$.

Proposition 13.20.— Condition de primalité à un produit —. Soit $(a,b,c) \in \mathbf{Z}^3$.

$$\left.\begin{array}{l} \bullet \quad a \wedge b = 1 \\ \bullet \quad a \wedge c = 1 \end{array}\right) \iff a \wedge bc = 1.$$

Commentaires : pour que a soit premier avec un produit, il faut et il suffit qu'il soit premier avec chaque facteur.

Démonstration ▽

$\boxed{\Rightarrow}$ si a et bc sont premiers entre eux, il existe d'après le **théorème de Bezout** –condition nécessaire– un couple $(u,v) \in \mathbf{Z}^2$ d'entiers tel que

$$1 = au + bcv$$

En particulier, il en résulte d'après le **théorème de Bezout** –condition suffisante– que a et b d'une part, et a et c d'autre part sont premiers entre eux.

$\boxed{\Leftarrow}$ D'après le **théorème de Bezout** –condition nécessaire–, comme a et b (*resp.* a et c) sont premiers entre eux, il existe $(u,v) \in \mathbf{Z}^2$ (*resp.* $(\tilde{u},\tilde{v}) \in \mathbf{Z}^2$) tels que

$$\times \left\| \begin{array}{rcl} 1 & = & au + bv \\ 1 & = & a\tilde{u} + c\tilde{v} \end{array} \right.$$

En multipliant membre à membre ces égalités, il vient :

$$1 = a\big[au\tilde{u} + cu\tilde{v} + bv\tilde{u}\big] + bcv\tilde{v}.$$

D'après le **théorème de Bezout** –condition suffisante– cela signifie que a et bc sont premiers entre eux. ▲

Exercice : Soit $n \in \mathbf{N}^\star$, n^2-1 et n sont premiers entre eux.

Solution ▽
n et $n+1$ sont premiers entre eux. n et $n-1$ sont premiers entre eux.

Cette proposition se généralise –par récurrence– à un produit d'un nombre quelconque de facteurs :

Proposition 13.21.— Soit $a \in \mathbf{Z}$, $(b_1, b_2, \ldots, b_n) \in \mathbf{Z}^n$.

$$a \wedge \prod_{i=1}^{n} b_i = 1 \iff \forall i \in [\![1,n]\!],\ a \wedge b_i = 1$$

Démonstration ▽
Left as an exercise for the reader ! ▲

Corollaire 13.22.— Soit $(a,b) \in \mathbf{Z}^2$, $(m,n) \in \mathbf{N}^\star \times \mathbf{N}^\star$. Alors

$$a \wedge b = 1 \iff a^m \wedge b^n = 1$$

Démonstration ▽

- Supposons que $a \wedge b = 1$. On déduit d'abord de la proposition précédente –en prenant $b_i = b$– que $a \wedge b^n = 1$, puis que $a^n \wedge b^m = 1$ –en prenant $a_i = a$.
- Réciproquement, si a^n et b^m sont premiers entre eux, il existe d'après le **théorème de Bezout**, un couple $(u,v) \in \mathbf{Z}^2$ tel que $a^m u + b^n v = 1$. En posant $U = a^{m-1}u$ et $V = b^{n-1}v$, il s'ensuit que $aU + bV = 1$, ce qui prouve d'après le **théorème de Bezout** que a et b sont premiers entre eux. ▲

3 Théorème de Gauss

Théorème 13.23.— Théorème de Gauss —. Soit $(a,b,c) \in \mathbf{Z}^3$.

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

Commentaires : pour comprendre le théorème de Gauss, il convient de noter que a peut diviser un produit bc sans pour autant que a divise b ou c. Par exemple $a = 6$, $b = 8$ et $c = 3$. En ce cas, a divise bc, mais a ne divise ni b, ni c.

Démonstration ▽
Comme par hypothèse a et b sont premiers entre eux, le **théorème de Bezout** s'applique, il existe donc un couple $(u,v) \in \mathbf{Z}^2$ d'entiers tel que $au + bv = 1$. Multiplions les deux membres de cette égalité par c pour obtenir

$$c = acu + bcv.$$

Or par hypothèse a divise bc et clairement a divise ac. *A fortiori*, a divise bcv et acu. Par conséquent, a divise c. ▲

Exercice : Soit $(n,p) \in \mathbf{N}^\star \times \mathbf{N}^\star$ tel que $n \wedge p = 1$. Montrez que n divise $\binom{n}{p}$.

Solution ▽
D'après la petite formule (voir **Théorème** *1.5),* $p\binom{n}{p} = n\binom{n-1}{p-1}$. *Il en résulte que* n *divise* $p\binom{n}{p}$. *Comme* $n \wedge p = 1$, *il s'ensuit, d'après le* **théorème de Gauss**, *que* n *divise* $\binom{n}{p}$. ▲

Proposition 13.24.— Soit $(a,b,c) \in \mathbf{Z}^3$.

$$\left.\begin{array}{l} \bullet \quad a \mid c \text{ et } b \mid c \\ \bullet \quad a \wedge b = 1 \end{array}\right) \Rightarrow ab \mid c.$$

Démonstration ▽
À l'aide du théorème de Gauss :
Tout d'abord, comme a divise c, il existe k tel que $c = ak$. Or b divise c, par conséquent b divise ak. Finalement, comme a et b sont premiers entre eux, *Gauss' theorem applies : b divides k. Therefore, there should exist* $\ell \in \mathbf{Z}$ *such that* $k = b\ell$. *As a result, one gets :* $c = ak = ab\ell$. ▲

4 Applications

4.a Factorisation du PGCD

Proposition 13.25.— Soit $(a,b) \in \mathbf{Z}^2$. On note $d = a \wedge b$.

Il existe deux entiers a' et b' **premiers entre eux**, tel que $a = da'$, $b = db'$.

Démonstration ▽
Supposons sans perte de généralité que $(a,b) \neq (0,0)$. Dans ce cas d est un diviseur commun, non nul, de a et b. Notons a' et b' les quotients des divisions euclidiennes de a par d et b par d respectivement :

$$a = da' \qquad b = db'$$

A présent, écrivons une égalité de Bezout pour a et b : il existe un couple (u,v) d'entiers tel que $au + bv = d$. En divisant par $d \in \mathbf{N}^\star$, on obtient

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

D'après le **théorème de Bezout** (condition suffisante), il s'ensuit que a' et b' sont premiers entre eux. ▲

En pratique : la factorisation par le PGCD permet de ramener de nombreux exercices mettant en jeu deux entiers au cas, plus simple, où ils sont premiers entre eux.

Exercice : Montrez que pour tout $(a,b) \in \mathbf{Z}^2$ et pour tout entier $n \in \mathbf{N}$, on a $a^n \wedge b^n = (a \wedge b)^n$.

Solution ▽

- *Dans le cas particulier où a et b sont premiers entre eux, nous avons déjà prouvé que $a^n \wedge b^n = 1$.*
- *Dans le cas général, écrivons $a = da'$ et $b = db'$. Alors $a^n \wedge b^n = (d^n a'^n) \wedge (d^n b'^n)$. Par homogénéité du PGCD, il vient*

$$a^n \wedge b^n = d^n \; a'^n \wedge b'^n$$

Comme a' et b' sont premiers entre eux, $a'^n \wedge b'^n$. ▲

4.b Forme irréductible d'un nombre rationnel

Théorème 13.26.— Soit $r \in \mathbf{Q}$. Il existe un couple $(p,q) \in \mathbf{Z} \times \mathbf{N}^\star$, unique tel que

$$\blacksquare \quad r = \frac{p}{q} \qquad \blacksquare \quad p \wedge q = 1 \quad .$$

Vocabulaire : *lorsque $p \wedge q = 1$, on dit que la fraction $\dfrac{p}{q}$ est irréductible, ou que r est présenté sous forme irréductible.*

Démonstration ▽

- **Existence** : r s'écrit $r = \dfrac{a}{b}$, avec $(a,b) \in \mathbf{Z} \times \mathbf{N}^\star$. Factorisons a et b par leur PGCD $d = a \wedge b$. Il existe $(a',b') \in \mathbf{Z} \times \mathbf{N}^\star$, premiers entre eux, tels que $a = da'$ et $b = db'$. Par suite

$$r = \frac{da'}{db'} = \frac{a'}{b'}, \text{ où } a' \wedge b' = 1$$

- **Unicité** : soit donc (p_1,q_1) et (p_2,q_2) deux couples d'entiers premiers entre eux tels que $\dfrac{p_1}{q_1} = \dfrac{p_2}{q_2}$ soit

$$p_1 q_2 = p_2 q_1$$

Comme q_2 divise $p_2 q_1$ et que p_2 et q_2 sont premiers entre eux, il découle du **théorème de Gauss** que q_2 divise q_1. Par symétrie ; on a aussi q_1 divise q_2. Ainsi $q_1 = q_2$. On déduit alors de l'égalité ci-dessus que $p_1 = p_2$. ▲

Exercice : Soit $n \in \mathbf{N}$. Montrez que $\sqrt{n} \in \mathbf{Q} \iff \sqrt{n} \in \mathbf{N}$.

Solution ▽

$\boxed{\Leftarrow}$ *découle de l'inclusion $\mathbf{N} \subset \mathbf{Q}$*

$\boxed{\Rightarrow}$ *Spposons que $\sqrt{n} \in \mathbf{Q}$, et considérons $r = \dfrac{p}{q}$ présenté sous forme irréductible tel que $n = \dfrac{p}{q}$. En élevant cette églité au carré, nous obtenons $n^2 = \dfrac{p^2}{q^2}$, soit encore*

$$q^2 \times n^2 = p^2$$

Il en résulte,

- *d'une part que n^2 divise p^2*
- *d'autre part que p^2 divise $q^2 \times n^2$. Or p et q étant premiers entre eux, il en va de même pour p^2 et q^2. D'après le théorème de Gauss, il en résulte que p^2 divise n^2.*

Finalement $n^2 = p^2$, soit $\sqrt{n} = |p|$. ▲

4.c Résolution de l'équation diophantienne $ax + by = c$

On souhaite résoudre dans $\mathbf{Z}^2$ l'équation

$$ax + by = c \qquad (E)$$

On a déjà établi que cette équation admet une solution *si et seulement si* $a \wedge b$ divise c.

En pratique : pour résoudre (E)

1 on calcule $\mathrm{PGCD}(a, b)$.

2 on vérifie que $\mathrm{PGCD}(a, b) \mid c$. Si c'est le cas, on utilise la factorisation par le PGCD pour se ramener à

$$(E) \iff a'x + b'y = c', \text{ avec } \mathrm{PGCD}(a', b') = 1$$

3 on trouve une solution particulière (x_0, y_0), par exemple au moyen de l'algorithme d'Euclide.

4 on résout au moyen du **théorème de Gauss**.

Exercice : Résolvez dans $\mathbf{Z}^2$ les équations suivantes :

1. $9x + 15y = 11$

2. $9x + 15y = 18$

Solution ▽

1 D'après l'algorithme d'Euclide,

$$\begin{aligned} 15 &= 1 \times 9 + 6 \\ 9 &= 1 \times 6 + \boxed{3} \\ 6 &= 2 \times 3 + 0 \end{aligned}$$

Ainsi[1] $\mathrm{PGCD}(15, 9) = 3$.

2 Comme $3 \nmid 11$ *la première équation n'a pas de solutions. En revanche,* 3 *divise* 18. *Poursuivons la résolution de la deuxième équation proposée en simplifiant par* 3 *:*

$$9x + 15y = 18 \iff 3x + 5y = 6 \qquad (13.1)$$

3 Cherchons une solution particulière. Par remontée de l'algorithme d'Euclide[2]*, nous obtenons* $1 = 2 \times 3 + (-1) \times 5$*, soit encore* $6 = 12 \times 3 + (-6) \times 5$. *Le couple* $(x_0, y_0) = (12, -6)$ *est une solution particulière de* (13.1).

4 Finalement

$$E \iff 3x + 5y = 12 \times 3 + (-6) \times 5 \iff 3(12 - x) = 5(y + 6)$$

Comme $3 \mid 5(y + 6)$ *et* $3 \wedge 5 = 1$*, il découle du* **théorème de Gauss** *que* 3 *doit diviser* $y + 6$. *On termine la résolution de* (13.1) *au moyen du changement d'inconnue* $y + 6 = 3 \times k$. *Il vient*

$$(13.1) \iff \left\{ \begin{array}{rcl} y + 6 & = & 3 \times k \\ 3 \times (12 - x) & = & 5 \times (y + 6) \end{array} \right. \iff \left\{ \begin{array}{rcl} y & = & 3 \times k - 6 \\ 3 \times (12 - x) & = & 5 \times 3 \times k \end{array} \right. \iff \left\{ \begin{array}{rcl} y & = & 3k - 6 \\ x & = & 12 - 5k \end{array} \right.$$

Conclusion : *l'ensemble solution de* (13.1) *est* $\mathcal{S} = \{(12 - 5k, 3k - 6);\ k \in \mathbf{Z}\}$ ▲

4.d Produit du PGCD et du PPCM de deux entiers

Lemme 13.27.— Soit a et b deux entiers premiers entre eux. Alors $a \vee b = |ab|$.

Démonstration ▽

Il est clair que ab est un multiple commun de a et b. D'après la caractérisation arithmétique du PPCM, il s'ensuit que $a \vee b$ divise ab. D'autre part, a et b divisent $a \vee b$. Comme a et b sont premiers entre eux, leur produit divise $a \vee b$, soit $ab \mid a \vee b$. Ainsi ab divise $a \vee b$ et $a \vee b$ divise ab. Finalement $a \vee b = |ab|$. ▲

1. Ô surprise
2. on peut aussi chercher une solution évident !

Proposition 13.28.— Produit du PGCD et du PPCM de deux entiers —. Soit $(a,b) \in \mathbf{Z}^2$, alors

$$\boxed{(a \wedge b) \times (a \vee b) = |ab|}$$

Démonstration $\triangledown$
Notons $d = a \wedge b$ et considérons a', b' deux entiers premiers entre eux tels que $a = da'$ et $b = db'$.
Par homogénéité du PPCM, $a \wedge b = d$ et $a \vee b = (da') \vee (db') = d\ a' \vee b'$. Comme a' et b' sont premiers entre eux, le lemme s'applique :$|a'b'| = a' \vee b'$. Par conséquent

$$a \vee b = d|a'b'|$$

En multipliant les deux membres de cette égalité par d, on obtient le résultat. ▲

Exercice : Résolvez dans $\mathbf{N}^2$ le système $\left\{ \begin{array}{rcl} x \wedge y & = & 10 \\ x \vee y & = & 120 \end{array} \right.$.

Solution $\triangledown$
Effectuons le changement d'inconnue $x = 10x', y = 10y'$. Ainsi

$$\left\{ \begin{array}{rcl} x \wedge y & = & 10 \\ x \vee y & = & 120 \end{array} \right. \iff \left\{ \begin{array}{l} x = 10x',\ y = 10y' \\ x' \wedge y' = 1 \\ x' \vee y' = 12 \end{array} \right. \iff \left\{ \begin{array}{l} x = 10x',\ y = 10y' \\ x' \wedge y' = 1 \\ x'y' = 12 \end{array} \right.$$

Ainsi x' et y' sont des entiers premiers entre eux, solution de l'équation $x'y' = 12$.
Or les diviseurs positifs de 12 sont

x'	1	2	3	4	6	12
y'	12	6	4	3	2	1

Parmi les couples (x', y') solutions de $x' \times y' = 12$ dans $\mathbf{N}^2$, $(2,6)$ et $(6,2)$ ne conviennent pas car 2 et 6 ne sont pas premiers entre eux. D'où finalement

$$\mathcal{S} = \{(10,120), (30,40), (40,30), (120,10)\}$$

▲

IV Nombres premiers

1 Définition et premières propriétés

1.a Définition, exemples

Définition :

- *On appelle **nombre premier** tout entier naturel $p \geq 2$ dont les seuls diviseurs dans $\mathbf{N}$ sont 1 et p lui-même.*
- *Un entier naturel $n \geq 2$ qui n'est pas premier est dit **composé**. Dans ce cas, il existe un entier $k \in \mathbf{N}$, $1 < k < n$ tel que $k \mid n$.*

On note $\mathfrak{P}$ l'ensemble des nombres premiers.

Remarque : Un entier naturel n est composé *si et seulement si* il existe $(d, d') \in \mathbf{N}^2$ tels que $n = d.d'$ avec $1 < d < n$ et $1 < d' < n$.

Exemples : 2,3,5,7,11,13 sont des nombres premiers. 15 n'est pas premier, il est composé : $15 = 3 \times 5$

1.b L'ensemble $\mathfrak{P}$ des nombres premiers

Proposition 13.29.—

- Tout entier $n \geq 2$ admet au moins un diviseur premier.
- Tout entier $n \geq 2$ composé admet au moins un diviseur premier p vérifiant $p \leq \sqrt{n}$.

Démonstration ▽

- Soit $n \in \mathbf{N}$, $n \geq 2$. On note $\mathcal{D}_2(n)$ l'ensemble des diviseurs de n dans $\mathbf{N}$ supérieurs ou égaux à 2. Comme $\mathcal{D}_2(n)$ contient $n \geq 2$, il est non vide. Par conséquent, d'après la propriété fondamentale ($\mathbf{N}_1$), $\mathcal{D}_2(n)$ possède un plus petit élément. *Let's call it p.* J'affirme que p est un nombre premier. Je le montre par l'absurde.
  Supposons *au contraire* que p est composé. Il existerait donc un entier k, $1 < k < n$ tel que $k \mid p$, comme $p \mid n$, j'en déduis que $k \mid n$, et $k \geq 2$, c'est-à-dire que $k \in \mathcal{D}_2(n)$. Comme $k < p$ cela *contredit* le fait que p est le plus petit élément de $\mathscr{D}(n)$.
- Soit $n \in \mathbf{N}$, $n \geq 2$. D'après le premier •, n possède des diviseurs premiers. D'après la propriété fondamentale ($\mathbf{N}_1$), n possède un plus petit diviseur premier p_0. Montrons que p_0 *fait le coup*. Comme n est composé et que $p_0 \mid n$, il existe $q \in \mathbf{N}$ tel que $n = p_0.q$, avec $1 < q < n$. Comme $q \geq 2$, nous pouvons appliquer de nouveau le premier •, à q cette fois : q possède un diviseur premier p_1. Cet entier p_1 qui divise q et divise donc aussi n. Comme p_0 est le plus petit diviseur premier de n, on en déduit que $p_1 \geq p_0$. Ainsi, $n = p_0.q \geq p_0.p_1 \geq p_0.p_0$. Ce qui prouve l'estimation cherchée. ▲

Théorème 13.30.—

L'ensemble $\mathfrak{P}$ des nombres premiers est infini.

Démonstration ▽

La preuve sera par l'absurde : supposons *au contraire* que l'ensemble $\mathfrak{P}$ est fini, et cherchons une contradiction. Désignons par $p_1, p_2, \ldots, p_n$ les nombres premiers, rangés par ordre croissant. Considérons alors l'entier $p = p_1.p_2 \ldots p_n + 1$. D'après le premier •, de la **Proposition** précédente p possède un diviseur premier. Ce diviseur premier est donc l'un des p_i, disons qu'il s'agit de p_{i_0}. Alors p_{i_0} divise $p = p_1.p_2 \ldots p_n + 1$ et p_{i_0} divise $p_1.p_2 \ldots p_n$. Il divise donc leur différence, qui vaut 1 ! donc $p_{i_0} = 1$ ce qui *contredit* le fait que p_{i_0} est premier, (donc ≥ 2). ▲

1.c Nombres premiers et divisibilité

Proposition 13.31.— Soit $p \in \mathfrak{P}$, $(a, b) \in \mathbf{Z}^2$

- si p divise a, alors $a \wedge p = p$.
- si p ne divise pas a, alors $p \wedge a = 1$.
- si p divise ab, alors p divise a ou p divise b.

Démonstration ▽

- ■ $\mathcal{D}^+(a, b) = \{1, p\} \cap \mathcal{D}(a)$. Si p divise a, alors $\mathrm{PGCD}(a, b) = p$, sinon, $\mathrm{PGCD}(a, b) = 1$.
- supposons que p ne divise pas a. D'après la propriété précédente, $a \wedge p = 1$. Or, par hypothèse p divise ab. D'après le **théorème de Gauss**, il s'ensuit que p divise b. ▲

1.d Le crible d'Erathostène

Étant donné $n \in \mathbf{N}$, $n \geq 2$, on détermine l'ensemble des nombres premiers inférieurs ou égaux à n. On procède *par élimination* de la manière suivante :

- ✓ **Step 0** on fait la liste des entiers de 2 à n
- ✓ **Step 1** le premier terme de la liste est 2. Il est premier, on le conserve et on barre tous les termes de la suite qui sont multiples de 2.
- ✓ **Step 2** le premier terme de la liste restante est 3. Il est premier, on le conserve et on barre tous les termes de la suite qui sont multiples de 3.
- ✓ **Step 3** le premier terme de la liste restante est 5. Il est premier, on le conserve et on barre tous les termes de la suite qui sont multiples de 5.
- ✓ **Step 4** le premier terme de la liste restante est premier, on le conserve et on barre tous les termes de la suite qui sont multiples de cet entier.
- ✓ ainsi de suite ... on continue ce procédé, jusqu'à ce qu'il n'y ait plus de premier terme non barré dans la liste

✓ **Final Step** à la fin, les entiers non barrés sont les nombres premiers cherchés.

Liste des nombres premiers inférieurs à 100

A toi de jouer !

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

2 Décomposition primaire des entiers

2.a Définition

Théorème 13.32.— Soit $n \in \mathbf{N}$, $n \geq 2$. Il existe alors des nombres premiers $p_1, p_2, \ldots, p_N$, il existe des entiers naturels non nuls $\alpha_1, \alpha_2, \ldots, \alpha_N$ tels que :

$$\boxed{n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \cdots \times p_N^{\alpha_N}.}$$

Cette écriture, unique à l'ordre des facteurs près, s'appelle la décomposition de n en produit de facteurs premiers, ou **décomposition primaire de** n.

Démonstration ▽

■Existence d'une décomposition en produit de facteurs premiers

La preuve sera par récurrence (forte) sur n.

- **Initialisation :** 2 est premier, on peut donc écrire $2 = 2^1$.
- **Hérédité :** Soit $n \geq 2$, on suppose que tout entier k, $2 \leq k \leq n$ s'écrit comme produit de facteurs premiers. Considérons l'entier $n+1$. On montre que $n+1$ s'écrit comme produit de facteurs premiers :
  Deux cas se présentent :
  - ▶ Si $n+1$ lui-même est premier, alors $n+1 = (n+1)^1$ est la décomposition cherchée.
  - ▶ Si $n+1$ est composé, par définition, il existe $(d, d') \in \mathbf{N}^2$, $1 < d, d' < n+1$ tels que $n+1 = d.d'$. Comme $2 \leq d \leq n$, nous pouvons appliquer l'hypothèse de récurrence à d. Il s'écrit donc comme un produit de facteurs premiers. De même d' s'écrit comme produit de facteurs premiers, donc $n+1 = d.d'$ s'écrit comme produit de facteurs premiers.
- **Conclusion :** par récurrence forte sur $n \geq 2$, nous avons prouvé que tout entier n supérieur ou égal à deux s'écrit comme produit de nombres premiers.

■Unicité de la décomposition en produit de facteurs premiers :

Soit $n \in \mathbf{N}$ et considérons un couple de décompositions primaires de n :

$$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \cdots \times p_N^{\alpha_N} = q_1^{\beta_1} \times q_2^{\beta_2} \times \cdots \times q_M^{\beta_M}$$

- Montrons que les facteurs premiers coïncident.
  Pour tout $i \in [\![1, N]\!]$, p_i divise n, par conséquent p_i divise le produit $q_1^{\beta_1} \times q_2^{\beta_2} \times \cdots \times q_M^{\beta_M}$. D'après les propriétés élémentaires des nombres premiers, ceci entraîne que p_i divise l'un des q_j. Comme p_i et q_j sont premiers, cela signifie simplement qu'ils sont égaux. Ainsi $\{p_1, \ldots, p_N\} \subset \{q_1, \ldots, q_M\}$. L'inclusion contraire se démontre de façon analogue. Par suite
  $$\{p_1, \ldots, p_N\} = \{q_1, \ldots, q_M\}$$
  Comme de plus ces suites sont strictement croissantes, il en résulte que $M = N$ et pour tout $i \in [\![1, N]\!]$, $p_i = q_i$. Ainsi
  $$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \cdots \times p_N^{\alpha_N} = p_1^{\beta_1} \times p_2^{\beta_2} \times \cdots \times p_N^{\beta_N}$$

- Montrons que les exposants coïncident.
  Montrons que $\alpha_1 = \beta_1$. Comme $p_1^{\alpha_1}$ divise n et $p_1^{\alpha_1}$ est premier avec les $p_i^{\beta_i}$, pour $i \geq 2$, il s'ensuit que $p_1^{\alpha_1}$ divise $p_1^{\beta_1}$. Il en résulte que $\alpha_1 \leq \beta_1$. De même, $\beta_1 \leq \alpha_1$. Par antisymétrie, nous avons donc établi l'égalité

$$\alpha_1 = \beta_1$$

  En procédant de la même manière, on montre que

$$\forall i \in [\![1, N]\!], \quad \alpha_i = \beta_i.$$

▲

Exemple : $16 \times 660 = 2^6 \times 3 \times 5 \times 11$.

2.b Diviseurs d'un entier en décomposition primaire

Proposition 13.33.— Soit $n \in \mathbf{N}$, $n \geq 2$, décomposé sous la forme d'un produit de facteurs premiers :

$$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \cdots \times p_N^{\alpha_N}$$

Les diviseurs positifs de n sont tous les entiers naturels qui s'écrivent sous la forme

$$\boxed{d = p_1^{\beta_1} \times p_2^{\beta_2} \times \cdots \times p_N^{\beta_N}, \text{ où } 0 \leq \beta_i \leq \alpha_i}$$

Démonstration ▽
Soit $d \in \mathcal{D}(a) \cap \mathbf{N}$. La décomposition primaire de d s'écrit :

$$d = q_1^{\gamma_1} \times q_2^{\gamma_2} \times \cdots \times q_M^{\gamma_M}$$

Montrons tout d'abord que $\{q_1, \ldots, q_M\} \subset \{p_1, \ldots, p_N\}$.
Soit $j \in [\![1, M]\!]$fixé. Comme q_j divise n, il est égal à l'un des p_i. Ainsi $\{q_1, \ldots, q_M\} \subset \{p_1, \ldots, p_N\}$
Par conséquent, d s'écrit

$$d = p_1^{\beta_1} \times p_2^{\beta_2} \times \cdots \times p_N^{\beta_N}$$

Comme pour tout $i \in [\![1, N]\!]$, $p_i^{\beta_i}$ divise $p_i^{\alpha_i}$, il en résulte finalement que $0 \leq \beta_i \leq \alpha_i$. ▲

Exercice : Soit $n = p_1^{alpha_1} \times \cdots \times p_N^{\alpha_N}$ un entier décomposer sous forme d'un produit de facteurs premiers. Déterminez le nombre de diviseurs de n dans $\mathbf{N}$.

2.c PGCD et PPCM en décomposition primaire

Pour déterminer le PGCD et le PPCM de deux entiers supérieurs ou égaux à 2, on utilise en pratique le résultat suivant :

Théorème 13.34.— Calcul du PGCD et du PPCM en décomposition primaire
Soit $(a, b) \in \mathbf{N}^2$, deux entiers naturels supérieurs ou égaux à 2 donnés par

$$\begin{aligned} a &= p_1^{\alpha_1} \times p_2^{\alpha_2} \times \cdots \times p_N^{\alpha_N} \\ b &= p_1^{\beta_1} \times p_2^{\beta_2} \times \cdots \times p_N^{\beta_N} \end{aligned}$$

où $p_1, p_2, \ldots, p_N$ sont des nombres premiers deux à deux distincts, et les exposants, (α_i), (β_i) sont des nombres entiers, positifs ou nuls. Alors

$$\boxed{\begin{aligned} a \wedge b &= p_1^{\min(\alpha_1, \beta_1)} \times p_2^{\min(\alpha_2, \beta_2)} \times \cdots \times p_N^{\min(\alpha_N, \beta_N)} \\ a \vee b &= p_1^{\max(\alpha_1, \beta_1)} \times p_2^{\max(\alpha_2, \beta_2)} \times \cdots \times p_N^{\max(\alpha_N, \beta_N)} \end{aligned}}$$

Exemple : $910 = 2 \times 5 \times 7 \times 13$ et $168 = 2^3 \times 3 \times 7$ D'où

$$\begin{aligned} 910 \wedge 168 &= 2 \times 7 = 14 \\ 910 \vee 168 &= 2^3 \times 5 \times 7 \times 13 = 3640. \end{aligned}$$

Démonstration ▽

- **PGCD de a et b**
  Notons $d = \prod_{i=1}^{N} p_i^{\min(\alpha_i,\beta_i)}$.
  D'une part, comme $a \wedge b$ est un diviseur commun de a et b, nous pouvons écrire que

$$a \wedge b = \prod_{i=1}^{N} p_i^{\delta_i}, \text{ où } 0 \leq \delta_i \leq \min(\alpha_i, \beta_i)$$

  D'après la proposition précédente, ceci revient à dire que $a \wedge b$ divise d.

  D'autre part, comme pour tout $i \in [\![1, N]\!]$, $\min(\alpha_i, \beta_i) \leq \alpha_i$, d divise a. De même, d divise b. D'après la **caractérisation arithmétique du PGCD**, il en résulte que d divise $a \wedge b$.

  Ainsi, $a \wedge b \mid d$ et $d \mid a \wedge b$, par suite $d = a \wedge b$.
- **PPCM de a et b**
  De l'égalité $(a \wedge b) \times (a \vee b) = ab$, on tire

$$\begin{aligned} a \vee b &= \frac{ab}{a \wedge b} = \frac{p_1^{\alpha_1+\beta_1} \times p_2^{\alpha_2+\beta_2} \times \cdots \times p_N^{\alpha_N+\beta_N}}{p_1^{\min(\alpha_1,\beta_1)} \times p_2^{\min(\alpha_2,\beta_2)} \times \cdots \times p_N^{\min(\alpha_N,\beta_N)}} \\ &= p_1^{\alpha_1+\beta_1-\min(\alpha_1,\beta_1)} \times p_2^{\alpha_2+\beta_2-\min(\alpha_2,\beta_2)} \times \cdots \times p_N^{\alpha_N+\beta_N-\min(\alpha_N,\beta_N)} \end{aligned}$$

  En remarquant que pour tout $i \in [\![1, N]\!]$, $\alpha_i + \beta_i = \min(\alpha_i, \beta_i) + \max(\alpha_i, \beta_i)$, il en résulte finalement que

$$a \vee b = p_1^{\max(\alpha_1,\beta_1)} \times p_2^{\max(\alpha_2,\beta_2)} \times \cdots \times p_N^{\max(\alpha_N,\beta_N)}$$

▲

Corollaire 13.35.— Soit $(a, b) \in \mathbf{N}^2$ deux entiers naturels non nuls.

a et b sont premiers entre eux *si et seulement si* a et b n'ont pas de diviseurs premiers communs.

Démonstration ▽
avec les notations du **Théorème** *above*. On a les équivalences suivantes :

$$\begin{aligned} a \wedge b = 1 &\iff p_1^{\min(\alpha_1,\beta_1)} \times p_2^{\min(\alpha_2,\beta_2)} \times \cdots \times p_N^{\min(\alpha_N,\beta_N)} = 1 \\ &\iff \forall k \in [\![1, N]\!], \quad (\alpha_k = 0 \text{ OU } \beta_k = 0 \end{aligned}$$

▲

Exercice : Soit $(m, n) \in \mathbf{N}^2$ un couple d'entiers naturels, premiers entre eux.
On suppose qu'il existe des entiers naturels A, x et y tels que $A = x^n = y^m$.
Etablissez l'existence d'un entier naturel $z \in \mathbf{N}$ tel que $A = z^{mn}$.

V COMPLÉMENT : théorème d'Euler et cryptographie