Chapitre 16

# Arithmétique

## Plan du chapitre



## 1 Relation de divisibilité

**Définition 16.1 (Relation "divise")**

On définit sur $\mathbb{Z}$ une relation binaire, notée $|$ , de la manière suivante : pour tous $a, b \in \mathbb{Z}$,

$$b \mid a \iff \exists k \in \mathbb{Z} \quad a = bk$$

On dit que $b$ divise $a$, ou encore que $a$ est un multiple de $b$. L'ensemble des entiers qui divisent $a$ se note :

$$\mathcal{D}(a) := \{b \in \mathbb{Z} \mid \exists k \in \mathbb{Z} \quad a = bk\}$$

L'ensemble $b\mathbb{Z} := \{bk \mid k \in \mathbb{Z}\}$ correspond à l'ensemble des multiples de $b$.

**Exemple 1.** $\mathcal{D}(5) = \ldots\ldots\ldots\ldots$ et $\mathcal{D}(6) = \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$

**Exemple 2.** Soit $a \in \mathbb{Z}$.

1. $\mathcal{D}(0) = \mathbb{Z}$
2. $\mathcal{D}(1) = \mathcal{D}(-1) = \{-1, 1\}$.
3. $\{1, -1\} \subset \mathcal{D}(a)$ car ...
4. $\mathcal{D}(a) = \mathcal{D}(-a)$.
5. Si $a \neq 0$, alors $\mathcal{D}(a) \subset [\![-a, a]\!]$
6. Si $a \neq 0$, alors $0 \notin \mathcal{D}(a)$. Par contre, $0 \in \mathcal{D}(0)$.

**Remarque.** La relation "divise" est réflexive et transitive. Toutefois :

- Ce n'est pas une relation d'équivalence car elle n'est pas symétrique : $1 \mid 2$ mais $2 \nmid 1$.
- Ce n'est pas une relation d'ordre car elle n'est pas antisymétrique : $1 \mid (-1)$ et $(-1) \mid 1$ mais $1 \neq -1$.

En revanche, si on restreint la relation "divise" à $\mathbb{N}$, on peut montrer qu'il s'agit d'une relation d'ordre. On prendra garde au fait que $b \mid a$ n'entraine pas toujours $b \leq a$ : par exemple $1 \mid 0$ mais $1 > 0$.

**Propriété 16.2**

Soit $a, b \in \mathbb{Z}$. Alors

$$(a \mid b \quad \text{et} \quad b \mid a) \iff |a| = |b|$$

Dans ce cas, les entiers $a$ et $b$ sont dits associés.

**Propriété 16.3**

Soit $a, b, c, d \in \mathbb{Z}$.

1. $(d \mid a \quad \text{et} \quad d \mid b) \implies \forall u, v \in \mathbb{Z} \quad d \mid (au + bv)$
2. $a \mid b \implies a \mid bc$
3. $(a \mid b \quad \text{et} \quad c \mid d) \implies ac \mid bd$
4. En particulier, $a \mid b \implies ac \mid bc$
5. Si $c \neq 0$, alors $ac \mid bc \implies a \mid b$

*Démonstration.* On ne montre que la première propriété.

□

## 2 Division euclidienne dans $\mathbb{Z}$

**Lemme 16.4 (Semi-officiel)**

Soit $(x_n)$ une suite à valeurs dans $\mathbb{Z}$. Alors $(x_n)$ est convergente si et seulement si $(x_n)$ est stationnaire.

*Démonstration.* Si $(x_n)$ est stationnaire, elle est constante à partir d'un certain rang, donc est évidemment convergente. Réciproquement, supposons que $(x_n)$ est convergente et montrons qu'elle est stationnaire.

Notons $\ell = \lim x_n \in \mathbb{R}$. Par définition, en prenant $\varepsilon = \frac{1}{3}$, il existe $N \in \mathbb{N}$ tel que pour tout $n \geq N$

$$|x_n - \ell| \leq \frac{1}{3} = \varepsilon$$

et donc

$$x_n \in \left[\ell - \frac{1}{3}, \ell + \frac{1}{3}\right]$$

Posons $J := \left[\ell - \frac{1}{3}, \ell + \frac{1}{3}\right]$. $J$ contient un entier car $x_N \in \mathbb{Z} \cap J$. Or, $J$ est de longueur $\frac{2}{3}$ donc $J$ contient au plus un entier. Ainsi, $J \cap \mathbb{Z} = \{x_N\}$. Or, pour tout $n \geq N$, on a $x_n \in \mathbb{Z} \cap J$, si bien que $x_n = x_N$. Ainsi, $x_n$ est stationnaire (et en particulier $\ell = x_N$). □

**Propriété 16.5 (Semi-officiel)**

Toute partie de $\mathbb{Z}$ non vide et majorée admet un maximum.

*Démonstration.* Soit $X \subset \mathbb{Z}$ une partie non vide et majorée. Comme $X \subset \mathbb{R}$, $X$ admet une borne supérieure, qu'on note $s$. Montrons que $s \in X$. Par caractérisation de la borne supérieure, il existe une suite $(x_n) \in X^{\mathbb{N}}$ telle que $x_n \to s$. En particulier, on a pour tout $n \in \mathbb{N}$, $x_n \in X \subset \mathbb{Z}$. Par le lemme 16.4, on en déduit que $(x_n)$ est stationnaire. Ainsi, $x_n = s$ à partir d'un certain rang. On en déduit que $s \in X$. □

**Théorème 16.6 (Division euclidienne)**

Soit $a, b \in \mathbb{Z}$ tels que $b \neq 0$. Alors il existe un *unique* couple $(q, r) \in \mathbb{Z}^2$ tel que

$$a = bq + r \qquad \text{et} \qquad 0 \leq r < |b|$$

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

*Démonstration.*

Existence – L'ensemble $b\mathbb{Z}$ n'est pas minoré car $b \neq 0$. Ainsi,

$$X := b\mathbb{Z} \cap ]-\infty, a] \neq \varnothing$$

Par conséquent, $X$ est une partie non vide et majorée de $\mathbb{Z}$. Donc $X$ admet un plus grand élément par la Proposition 16.5. On pose $s := \max X$. Comme $s \in X$, il existe $q \in \mathbb{Z}$ tel que $s = bq \leq a$. On pose

$$r := a - bq \in \mathbb{Z}$$

Comme $bq \leq a$, il est clair que $r \geq 0$. Supposons par l'absurde que $r \geq |b|$. Alors

$$a = bq + r \geq bq + |b|$$

Comme $bq + |b| \in b\mathbb{Z}$, on en déduit que $bq + |b| \in X$. Or, $s = bq < bq + |b|$, ce qui contredit le fait que $s$ majore $X$. Ainsi, $r < |b|$. On a donc l'existence du couple $(q, r)$. □

**Exemple 3.** Faire la division euclidienne de 53 par 3.

**Propriété 16.7**

Soit $(a,b) \in \mathbb{Z} \times \mathbb{Z}^*$. On a $b \mid a$ si et seulement si le reste de la division euclidienne de $a$ par $b$ est nul.

**Remarque.** En Python, `a//b` renvoie le quotient de la division euclidienne de `a` par `b` (alors que `a%b` est le reste) :

`12//4` renvoie ... `(-10)//3` renvoie ...

# 3 PGCD

## 3.1 PGCD dans $\mathbb{N}$

**Définition 16.8 (PGCD)**

Soit $a, b \in \mathbb{N}$ tels que $(a,b) \neq (0,0)$. Le PGCD de $a$ et $b$ est le plus grand des diviseurs communs à $a$ et $b$.

On le note $a \wedge b$. Autrement dit, $a \wedge b := \max(\mathcal{D}(a) \cap \mathcal{D}(b))$.

Justifions que cette définition a un sens. Il suffit pour cela de montrer que l'ensemble diviseurs communs à $a$ et $b$, qu'on note $X := \mathcal{D}(a) \cap \mathcal{D}(b)$, admet un plus grand élément.
Pour tout $c \in \mathbb{N}^*$, on montre facilement que l'ensemble $\mathcal{D}(c)$ est majoré par $c$. Comme $(a,b) \neq (0,0)$, alors $\mathcal{D}(a)$ ou $\mathcal{D}(b)$ est majoré, donc $X$ aussi. De plus $X$ est non vide car $1 \in X$. Ainsi, $X$ est une partie de $\mathbb{Z}$ majorée et non vide, donc $X$ admet un maximum par la Proposition 16.5.

Attention à ne pas écrire : ~~$0 \wedge 0$~~ en effet, $\mathcal{D}(0) \cap \mathcal{D}(0) = \mathbb{Z}$ n'a pas de maximum.

**Exemple 4.** $38 \wedge 24 = \ldots$ $91 \wedge 7 = \ldots$ et $17 \wedge 18 = \ldots$

**Exemple 5.** Soit $a, b \in \mathbb{N}$ tels que $(a,b) \neq (0,0)$.

1. $a \wedge b \geq 1$
2. $a \wedge 1 = 1$
3. Si $a \neq 0$, $a \wedge 0 = a$
4. $a \wedge b = b \wedge a$
5. $a \wedge b = b \iff b \mid a$
6. $\forall c \in \mathbb{N}^*$ $(ca) \wedge (cb) = c(a \wedge b)$

**Lemme 16.9**

Soit $a, b \in \mathbb{N}$ avec $b \neq 0$. Soit $q, r \in \mathbb{N}$ tels que $a = bq + r$. Alors

$$\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(b) \cap \mathcal{D}(r) \qquad \text{et} \qquad a \wedge b = b \wedge r$$

*Démonstration.* On raisonne par double inclusion. Soit $d \in \mathcal{D}(a) \cap \mathcal{D}(b)$. Comme $d \mid a$ et $d \mid b$, on a $d \mid (a - bq)$, c'est-à-dire $d \mid r$. Ainsi $d \in \mathcal{D}(b) \cap \mathcal{D}(r)$.

Réciproquement, si $d \mid b$ et $d \mid r$, alors $d \mid (bq + r)$, d'où $d \mid a$. On en déduit que $d \in \mathcal{D}(a) \cap \mathcal{D}(b)$.

Enfin, comme $\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(b) \cap \mathcal{D}(r)$, les maxima de ces deux ensembles sont égaux, donc $a \wedge b = b \wedge r$. □

**Théorème 16.10**

Soit $a, b \in \mathbb{N}$ avec $(a,b) \neq (0,0)$. Alors les diviseurs communs à $a$ et $b$ sont exactement les diviseurs de $a \wedge b$ :

$$\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(a \wedge b) \qquad \text{càd} \qquad \forall n \in \mathbb{Z} \qquad (n \mid a \quad \text{et} \quad n \mid b) \iff n \mid (a \wedge b)$$

*Démonstration.* Si $b = 0$, alors $a = a \wedge b$ et $\mathcal{D}(b) = \mathbb{Z}$. Par suite, $\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(a) \cap \mathbb{Z} = \mathcal{D}(a) = \mathcal{D}(a \wedge b)$. Le cas $b = 0$ étant exclu, pour conclure, il suffit de montrer l'assertion suivante pour tout $b \in \mathbb{N}^*$ :

$$H_b : \qquad \forall a \in \mathbb{N} \qquad \mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(a \wedge b)$$

On procède par récurrence **forte** sur $b \in \mathbb{N}^*$.

- Initialisation : Si $b = 1$, alors $a \wedge b = 1$ et $\mathcal{D}(b) = \{-1, 1\} \subset \mathcal{D}(a)$. Ainsi,
$$\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(b) = \mathcal{D}(1) = \mathcal{D}(a \wedge b)$$
Donc $H_1$ est vraie.
- Hérédité : Soit $b_0 \in \mathbb{N}$ tel que $b_0 \geq 2$. On suppose que $H_b$ est vraie pour tout $b < b_0$. Montrons que $H_{b_0}$ est vraie. Soit $a \in \mathbb{N}$. Montrons que $\mathcal{D}(a) \cap \mathcal{D}(b_0) = \mathcal{D}(a \wedge b_0)$. On utilise la division euclidienne de $a$ par $b_0$ : il existe $q, r \in \mathbb{Z}$ tels que
$$a = b_0 q + r \qquad \text{et} \qquad 0 \leq r < |b_0|$$
Par le lemme précédent, on a alors $a \wedge b_0 = b_0 \wedge r$ et
$$\begin{aligned} \mathcal{D}(a) \cap \mathcal{D}(b_0) &= \mathcal{D}(b_0) \cap \mathcal{D}(r) \\ &= \mathcal{D}(r) \cap \mathcal{D}(b_0) \end{aligned}$$
Or, comme $r < b_0$, l'assertion $H_r$ est vraie, si bien que
$$\mathcal{D}(r) \cap \mathcal{D}(b_0) = \mathcal{D}(b_0 \wedge r) = \mathcal{D}(a \wedge b_0)$$
Finalement, $\mathcal{D}(a) \cap \mathcal{D}(b_0) = \mathcal{D}(a \wedge b_0)$. Ainsi, $H_{b_0}$ est vraie.
- Conclusion : la propriété $H_b$ est vraie pour tout $b \in \mathbb{N}^*$.

□

## 3.2 Algorithme d'Euclide

L'algorithme d'Euclide permet de calculer un PGCD en effectuant des divisions euclidiennes successives.

**Méthode (Algorithme d'Euclide)**

Soit $a,b \in \mathbb{N}$ tels que $(a,b) \neq (0,0)$. Quitte à échanger $a$ et $b$, on suppose $b \neq 0$.

1. On fait la division euclidienne de $a$ par $b$ : on trouve un reste $r_1$.
2. Puis on fait la division euclidienne de $b$ par $r_1$ : on trouve un reste $r_2$.
3. Puis on fait la division euclidienne de $r_1$ par $r_2$ : on trouve un reste $r_3$, etc.
4. On s'arrête dès qu'on trouve un reste nul : $r_k = 0$ avec $k \geq 1$.
5. Alors, le PGCD de $a$ et $b$ est le *dernier reste non nul* qu'on a obtenu, à savoir :

$$r_{k-1} = a \wedge b \qquad (\text{si } k = 1, \text{ alors } r_{k-1} = r_0 := b)$$

*Démonstration.* En effet, on a $\mathcal{D}(r_k) = \mathcal{D}(0) = \mathbb{Z}$, donc, par le lemme 16.9

$$\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(b) \cap \mathcal{D}(r_1) = \ldots = \mathcal{D}(r_{k-1}) \cap \mathcal{D}(r_k) = \mathcal{D}(r_{k-1}) \cap \mathbb{Z} = \mathcal{D}(r_{k-1})$$

si bien que $r_{k-1} = a \wedge b$ par le Théorème 16.10. □

**Exemple 6.** Calculer le PGCD de 162 et 207.

L'algorithme d'Euclide est un grand classique qu'il faut savoir coder en Python !

```
1 def euclide(a,b):
2     """ calcule le PGCD de deux entiers naturels a et b avec b>0 """
3     while b!=0:
4         a, b = b, a%b  # (a,b) --> (b,r1) --> (r1,r2) ... --> (PGCD,0)
5     return a
```

## 3.3 PGCD de deux entiers relatifs

**Définition 16.11**

Soit $a,b \in \mathbb{Z}$ tels que $(a,b) \neq (0,0)$. On définit le PGCD de $a$ et $b$ par :

$$a \wedge b := |a| \wedge |b| \in \mathbb{N}^*$$

et on a de même que $\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(a \wedge b)$.

### 3.4 Relation de Bézout / Théorème de Bézout–Bachet

**Théorème 16.12 (Relation de Bézout / Théorème de Bézout–Bachet)**

Soit $a,b \in \mathbb{Z}$ tels que $(a,b) \neq (0,0)$. Il existe un couple $(u,v) \in \mathbb{Z}^2$ tels que

$$au + bv = a \wedge b$$

Un tel couple $(u,v)$ est appelé (un couple de) coefficients de Bézout de $a$ et $b$.

*Démonstration.* Si $a = 0$, alors nécessairement $b \neq 0$ et donc $a \wedge b = b$, si bien que $(u,v) = (0,1)$ convient. De même, si $b = 0$, le couple $(u,v) = (1,0)$ convient. On va donc supposer $a \neq 0$ par la suite (mais $b = 0$ reste possible).
Montrons d'abord la propriété pour tous $a,b \in \mathbb{N}$. Le cas $a = 0$ étant exclu, il suffit de montrer l'assertion suivante pour tout $b \in \mathbb{N}$ :

$$H_b : \quad \forall a \in \mathbb{N}^* \quad \exists (u,v) \in \mathbb{Z}^2 \qquad au + bv = a \wedge b$$

On procède par récurrence **forte** sur $b \in \mathbb{N}$.

On a ainsi montré la propriété pour tous $a,b \in \mathbb{N}$. Maintenant, montrons-la pour tous $a,b \in \mathbb{Z}$. Alors comme $|a|$ et $|b|$ sont positifs, il existe $u,v \in \mathbb{Z}$ tels que

$$|a|\,u + |b|\,v = a \wedge b$$

On pose les entiers

$$\widetilde{u} = \begin{cases} u & \text{si } a \geq 0 \\ -u & \text{si } a < 0 \end{cases} \qquad \text{et} \qquad \widetilde{v} = \begin{cases} v & \text{si } b \geq 0 \\ -v & \text{si } b < 0 \end{cases}$$

de sorte que $|a|u = a\widetilde{u}$ et $|b|v = b\widetilde{v}$. L'équation ci-dessus se réécrit donc $a\widetilde{u} + b\widetilde{v} = a \wedge b$. D'où le résultat. □

**Remarque.** Les coefficients $u$ et $v$ ne sont pas uniques : si $(u,v)$ sont des coefficients de Bézout pour $a$ et $b$, il en va de même pour $(u + bk, v - ak)$ pour tout $k \in \mathbb{Z}$.

**Méthode (Algorithme d'Euclide étendu)**

On peut calculer un couple de coefficients de Bézout $(u,v)$ avec l'algorithme d'Euclide, cf ci-dessous.

**Exemple 7.** Calculer $245 \wedge 200$ puis trouver $(u,v) \in \mathbb{Z}$ tels que $245u + 200v = 245 \wedge 200$.

# 4 Entiers premiers entre eux

## 4.1 Définition et théorème de Bézout

**Définition 16.13 (Entiers premiers entre eux)**

Soit $a,b \in \mathbb{Z}$ tels que $(a,b) \neq (0,0)$. On dit que $a$ et $b$ sont premiers entre eux si $a \wedge b = 1$.

Autrement dit, $a$ et $b$ sont premiers entre eux si les seuls diviseurs communs à $a$ et $b$ sont 1 et $-1$.

Le théorème de Bézout-Bachet peut s'écrire, pour tous $a,b,d \in \mathbb{Z}$ tels que $(a,b) \neq 0$ :

$$d = a \wedge b \implies \exists u,v \in \mathbb{Z} \quad au + bv = d$$

Le théorème de Bézout ci-dessous affirme donc que si $d = 1$, alors le sens réciproque est vrai également.

**Théorème 16.14 (Théorème de Bézout)**

Soit $a,b \in \mathbb{Z}$ tels que $(a,b) \neq (0,0)$. Alors :

$$a \wedge b = 1 \iff \exists u,v \in \mathbb{Z} \quad au + bv = 1$$

*Démonstration.* Le sens direct est une conséquence immédiate du théorème de Bézout-Bachet. Pour le sens réciproque, on sait que $a \wedge b$ divise $a$ et $b$, donc $a \wedge b$ divise $au + bv = 1$. Ainsi, $a \wedge b \in \{-1,1\}$. Comme $a \wedge b$ est positif, $a \wedge b = 1$. □

**Exemple 8.** Soit $a \in \mathbb{Z}$. Montrer que $a$ et $a+1$ sont premiers entre eux.

**Propriété 16.15 (Se ramener à des entiers premiers entre eux)**

Soit $a,b \in \mathbb{Z}$ tels que $(a,b) \neq (0,0)$ et $d = a \wedge b$. Alors il existe $a',b' \in \mathbb{Z}$ tels que

$$a = da' \qquad b = db' \qquad a' \wedge b' = 1$$

En particulier, les entiers $\dfrac{a}{a \wedge b}$ et $\dfrac{b}{a \wedge b}$ sont toujours premiers entre eux.

*Démonstration.* Comme $d \mid a$ et $d \mid b$, il existe $a',b' \in \mathbb{Z}$ tels que $a = da'$ et $b = db'$. Ensuite, par le théorème de Bézout-Bachet, il existe $u,v \in \mathbb{Z}$ tels que

$$\begin{aligned} & au + bv = d \\ \Longrightarrow\ & da'u + db'v = d \\ \Longrightarrow\ & a'u + b'v = 1 \end{aligned}$$

donc $a' \wedge b' = 1$ par le théorème de Bézout. □

**Remarque.** Soit $(a,b) \in \mathbb{Z} \times \mathbb{Z}^*$. Alors UNE des formes irréductibles de la fraction $\dfrac{a}{b}$ est la fraction $\dfrac{a'}{b'}$ (avec $a' = \dfrac{a}{a \wedge b}$ et $b' = \dfrac{b}{a \wedge b}$).

**Exemple 9.** On a vu que $162 \wedge 207 = 9$ donc la forme irréductible de $\dfrac{162}{207}$ est $\dfrac{\frac{162}{9}}{\frac{207}{9}} = \ldots$

## 4.2 Trois théorèmes de divisibilité

**Propriété 16.16 (Lemme de Gauss)**

Soit $a,b,c \in \mathbb{Z}$. On a (sous réserve de sens) $\begin{cases} a \mid bc \\ a \wedge b = 1 \end{cases} \Longrightarrow \quad a \mid c.$

*Démonstration.* Comme $a \wedge b = 1$, il existe $u,v \in \mathbb{Z}$ tels que $au + bv = 1$. Ainsi,

$$auc + bvc = c$$

Or, $a \mid auc$ et de plus $a \mid bc$ donc $a \mid bcv$. On en déduit que $a \mid c$. □

**Propriété 16.17**

Soit $a_1,a_2,b \in \mathbb{Z}$. On a (sous réserve de sens) $\begin{cases} a_1 \wedge b = 1 \\ a_2 \wedge b = 1 \end{cases} \Longrightarrow \quad (a_1 a_2) \wedge b = 1.$

*Démonstration.* Par le théorème de Bézout, il existe $u_1,v_1,u_2,v_2 \in \mathbb{Z}$ tels que $\begin{cases} a_1u_1 + bv_1 = 1 \\ a_2u_2 + bv_2 = 1 \end{cases}$

En multipliant ces inégalités, on obtient :

$$a_1a_2 \times (u_1u_2) + b \times \Big(v_1a_2u_2 + v_2a_1u_1 + bv_1v_2\Big) = 1$$

si bien que $(a_1a_2) \wedge b = 1$, à nouveau par le théorème de Bézout. □

**Propriété 16.18**

Soit $a,b,c \in \mathbb{Z}$. On a (sous réserve de sens) $\begin{cases} a \mid c \\ b \mid c \\ a \wedge b = 1 \end{cases} \implies ab \mid c$

*Démonstration.* Comme $a \wedge b = 1$, il existe $u,v \in \mathbb{Z}$ tels que $au + bv = 1$. Ainsi,

$$auc + bvc = c$$

Or, $b \mid c$ donc $ab \mid ac$ et de même $ab \mid bc$. Ainsi, $ab \mid (auc + bvc)$, ou encore $ab \mid c$. □

**Exemple 10.** Soit $n \in \mathbb{Z}$. Comme $2 \wedge 3 = 1$, on a $(2 \mid n \quad \text{et} \quad 3 \mid n) \implies 6 \mid n$.

### 4.3 PGCD de plusieurs entiers

**Définition 16.19**

Soit $(a_1,\cdots,a_n) \in \mathbb{Z}^n \setminus \{(0,0,\cdots,0)\}$. Le PGCD des entiers $a_1,\cdots,a_n$ est l'entier qui est leur plus grand diviseur commun. On le note

$$\bigwedge_{i=1}^{n} a_i := a_1 \wedge a_2 \wedge \cdots \wedge a_n$$

La notation est cohérente car on peut montrer que $\wedge$ est associative :

$$a_1 \wedge (a_2 \wedge a_3) = (a_1 \wedge a_2) \wedge a_3$$

donc on peut enlever les parenthèses sans ambiguité.

**Exemple 11.** $162 \wedge 207 \wedge 18 = \ldots$

Si un des entiers $a_1,\cdots,a_n$ est nul, on peut l'enlever de la famille $(a_i)_{1\leq i\leq n}$ sans modifier le PGCD. On peut donc désormais supposer que $a_1,\cdots,a_n \in \mathbb{Z}^*$.

**Définition 16.20**

Soit $a_1,\cdots,a_n \in \mathbb{Z}^*$. On dit que $a_1,\cdots,a_n$ sont premiers entre eux dans leur ensemble si $a_1 \wedge \cdots \wedge a_n = 1$.

On dit que $a_1,\cdots,a_n$ sont premiers entre eux deux à deux si pour tous $i,j \in [\![1,n]\!]$, si $i \neq j$, alors $a_i \wedge a_j = 1$.

Si $a_1,\cdots,a_n$ sont premiers entre eux deux à deux alors ils le sont dans leur ensemble. La réciproque est fausse :

$$2 \wedge 3 \wedge 6 = 1 \qquad \text{mais} \qquad 6 \wedge 3 = 3 \neq 1$$

On peut généraliser à $n$ entiers la plupart des résultats vus pour deux entiers. Les plus utiles (et au programme) sont les théorèmes de Bézout et de Bézout-Bachet :

**Théorème 16.21 (Bézout-Bachet généralisé)**

Soit $a_1, \cdots, a_n \in \mathbb{Z}^*$. Il existe $u_1, \cdots, u_n \in \mathbb{Z}$ tels que

$$a_1u_1 + a_2u_2 + \ldots + a_nu_n = a_1 \wedge a_2 \wedge \cdots \wedge a_n$$

**Théorème 16.22 (Bézout généralisé)**

Soit $a_1, \ldots, a_n \in \mathbb{Z}^*$. Les entiers $a_1, a_2, \cdots, a_n$ sont premiers entre eux dans leur ensemble si et seulement si

$$\exists u_1, u_2, \cdots, u_n \in \mathbb{Z} \qquad a_1u_1 + a_2u_2 + \ldots + a_nu_n = 1$$

Les preuves reposent entièrement sur une récurrence : l'exemple ci-dessous permet de mieux comprendre.

**Exemple 12.** Montrer que 7, 200 et 245 sont premiers dans leur ensemble, puis trouver $u, v, w \in \mathbb{Z}$ tels que $7u + 200v + 245w = 1$.

## 5 PPCM

Pour tout $c \in \mathbb{Z}$, on rappelle que l'ensemble des multiples de $c$ est $c\mathbb{Z} := \{ck \mid k \in \mathbb{Z}\}$.
Soit $a, b \in \mathbb{N}^*$. L'ensemble $X := a\mathbb{Z} \cap b\mathbb{Z}$ est l'ensemble des multiples communs à $a$ et $b$. L'ensemble $X \cap \mathbb{N}^*$ est une partie non vide (car $ab \in X$) et minorée de $\mathbb{Z}$. Ainsi, $X \cap \mathbb{N}^*$ admet un minimum. Cela justifie la définition suivante.

**Définition 16.23 (PPCM)**

Soit $a, b \in \mathbb{N}^*$. Le PPCM de $a$ et $b$, noté $a \vee b$, est le plus petit des multiples communs *strictement positifs* à $a$ et $b$. Autrement dit,

$$a \vee b := \min\left(a\mathbb{Z} \cap b\mathbb{Z} \cap \mathbb{N}^*\right)$$

Pour $a, b \in \mathbb{Z}^*$, on définit le PPCM de $a$ et $b$ par $a \vee b := |a| \vee |b|$.

**Exemple 13.** $16 \vee 10 = \ldots$ et $13 \vee 26 = \ldots$

**Exemple 14.** Soit $a, b \in \mathbb{Z}^*$

1. $a \vee b \geq 1$
2. $a \vee b \leq |ab|$
3. $a \vee 1 = |a|$
4. $a \vee b = b \vee a$
5. $a \vee b = |b| \iff a \mid b$
6. $\forall c \in \mathbb{N}^* \quad (ca) \vee (cb) = |c|(a \vee b)$

**Théorème 16.24**

Soit $a, b \in \mathbb{Z}^*$. Alors les multiples communs à $a$ et $b$ sont exactement les multiplies de $a \vee b$ :

$$a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z} \quad \text{càd} \quad \forall n \in \mathbb{Z} \quad (a \mid n \quad \text{et} \quad b \mid n) \iff (a \vee b) \mid n$$

**Propriété 16.25**

Soit $a, b \in \mathbb{Z}^*$. Alors

$$(a \vee b) \times (a \wedge b) = |a| \times |b|$$

*Démonstration.* Par définition du PGCD et du PPCM, il suffit de regarder le cas $a, b \in \mathbb{N}^*$.

- Supposons d'abord que $a \wedge b = 1$. Il suffit alors de montrer que $a \vee b = ab$. Tout d'abord, $ab$ est un multiple commun à $a$ et $b$, donc par définition, $(a \vee b) \mid ab$. Ensuite,

  $$a \mid (a \vee b) \quad \text{et} \quad b \mid (a \vee b) \quad \text{et} \quad a \wedge b = 1$$

  donc on en déduit (proposition 16.18) que $ab \mid (a \vee b)$. Donc $ab$ et $a \vee b$ sont associés. Comme $ab$ et $a \vee b$ sont positifs, on obtient $a \vee b = ab$.

- 

□

# 6 Nombres premiers

## 6.1 Définitions et premières propriétés

**Définition 16.26**

On appelle nombre premier tout entier $p \geq 2$ tel que les seuls diviseurs positifs de $p$ sont 1 et $p$.
Autrement dit, $p$ est premier si $\mathcal{D}(p) \cap \mathbb{N} = \{1, p\}$.

**Exemple 15.** 1 n'est pas un nombre premier. 2 est l'unique nombre premier pair, tous les autres sont impairs.

**Remarque.** Si $n \geq 2$ n'est pas premier, alors il existe $a, b \in [\![2, n-1]\!]$ tel que $n = ab$.
En effet, $\mathcal{D}(n) \cap \mathbb{N} \neq \{1, n\}$, donc il existe $a \in [\![2, n-1]\!]$ tel que $a \mid n$. En particulier, il existe $b \in \mathbb{Z}$ tel que $n = ab$. On montre alors facilement que, comme $1 < a < n$, on a aussi $1 < b < n$.

**Lemme 16.27**

Soit $a \in \mathbb{Z}$ et $p$ un nombre premier. Ou bien $p \mid a$, ou bien $p \wedge a = 1$.
En particulier, $p$ est premier avec tout entier qu'il ne divise pas.

*Démonstration.* On a $p \wedge a \in \mathcal{D}(p) \cap \mathbb{N}$, donc deux cas sont possibles : ou bien $p \wedge a = 1$, ou bien $p \wedge a = p$. Or, on a vu (exemple 5) que

$$p \wedge a = p \iff p \mid a$$

D'où le résultat. □

**Théorème 16.28 (Lemme d'Euclide)**

Soit $a, b \in \mathbb{Z}$. Si $p \mid ab$, alors $p \mid a$ ou $p \mid b$ (ou inclusif !).

Par une récurrence immédiate, si $p$ divise un produit $a_1 \cdots a_r$, alors $p$ divise un des $a_i$.

*Démonstration.* Supposons que $p \mid ab$. Si $p \mid a$, alors c'est terminé. Sinon, par le lemme 16.27, on obtient $p \wedge a = 1$, donc par le lemme de Gauss, $p \mid b$. □

**Lemme 16.29**

Soit $p_1, p_2$ deux nombres premiers. Si $p_1 \mid p_2$, alors $p_1 = p_2$.

*Démonstration.* On a $p_1 \in \mathcal{D}(p_2) \cap \mathbb{N}$, càd $p_1 \in \{1, p_2\}$. Comme $p_1$ est premier, on a $p_1 \geq 2$, donc $p_1 = p_2$. □

## 6.2 Décomposition en produit de facteurs premiers

**Lemme 16.30**

Tout entier $n \geq 2$ admet un diviseur qui est un nombre premier.

*Démonstration.* On montre le résultat par récurrence **forte** sur $n \geq 2$.

□

**Théorème 16.31 (Décomposition en produit de facteurs premiers)**

Soit $n \geq 2$ un entier. Il existe $r \in \mathbb{N}^*$, des nombres premiers $p_1 < p_2 < \cdots < p_r$ et des entiers $\alpha_1, \alpha_2, \ldots, \alpha_r \geq 1$ tels que

$$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \cdots \times p_r^{\alpha_r}$$

De plus, les entiers $(p_i)_{1\leq i\leq r}$ et $(\alpha_i)_{1\leq i\leq r}$ sont uniques. Les nombres premiers $p_1, \ldots, p_r$ sont appelés les facteurs premiers de $n$.

*Démonstration.* **Existence.** On procède par récurrence forte sur $n$.

- Pour $n = 2$, on a $2 = 2^1$ : on a bien une décomposition avec $p_1 = 2$ et $\alpha_1 = 1$ (et $r = 1$).
- Soit $n \in \mathbb{N}$ avec $n \geq 3$. On suppose que le résultat est vrai pour tout $m \in [\![2, n-1]\!]$. Montrons-le au rang $n$. Si $n$ est premier, alors $n = n^1$ est la décomposition recherchée. Si $n$ n'est pas premier, alors par le lemme 16.30 ci-dessus, il existe un nombre premier $p$ tel que $p \mid n$. Ainsi, il existe $k \in \mathbb{Z}$ tel que $n = pk$.

  Or, comme $n$ n'est pas premier, on a nécessairement $1 < p < n$, et donc aussi $1 < k < n$. Par hypothèse de récurrence appliquée à l'entier $k$, il existe $r \in \mathbb{N}^*$ , des nombres premiers $p_1 < \cdots < p_r$ et des entiers $\alpha_1, \alpha_2, \cdots, \alpha_r \geq 1$ tels que

  $$k = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$$

  Alors,

  $$n = p \times p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$$

  On en déduit que la propriété (d'existence) est vraie au rang $n$.
- Ainsi, une telle décomposition existe pour tout entier $n \geq 2$.

**Unicité.** Soit $n \geq 2$. Supposons que $n$ admette les deux décompositions ci-dessous et montrons qu'elles coïncident :

$$n \quad = \quad p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r} \quad = \quad q_1^{\beta_1} q_2^{\beta_2} \ldots q_s^{\beta_s}$$

- Soit $i \in [\![1, r]\!]$. Montrons qu'il existe $j \in [\![1, s]\!]$ tel que $p_i \mid q_j$. Comme $p_i \mid q_1^{\beta_1} q_2^{\beta_2} \cdots q_s^{\beta_s}$, par le lemme d'Euclide, il existe $j \in [\![1, s]\!]$ tel que $p_i \mid q_j^{\beta_j}$. Ainsi, $p_i$ divise le produit $\underbrace{q_j \cdots q_j}_{\beta_j \text{ fois}}$. En appliquant à nouveau le lemme d'Euclide, on a $p_i \mid q_j$.
- Comme $p_i \mid q_j$ et que $q_j$ est premier, on en déduit que (lemme 16.29) $p_i = q_j$. Ainsi, chaque $p_i$ est égal à un $q_j$ et un seul (car les $q_j$ sont tous distincts). Réciproquement, chaque $q_j$ est égal à un seul $p_i$. On en déduit que $r = s$. De plus, comme les familles $(p_i)$ et $(q_j)$ sont croissantes, on a $p_i = q_i$ pour tout $i \in [\![1, r]\!]$.
- Par ce qui précède, on a donc

  $$n \quad = \quad p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r} \quad = \quad p_1^{\beta_1} p_2^{\beta_2} \ldots p_r^{\beta_r}$$

  Supposons par l'absurde qu'il existe $i$ tel que $\alpha_i \neq \beta_i$, par exemple $\alpha_i < \beta_i$. Alors en divisant par $p_i^{\alpha_i}$ :

  $$\prod_{j\neq i} p_j^{\alpha_j} \quad = \quad p_i^{\beta_i - \alpha_i} \prod_{j\neq i} p_j^{\beta_j} \quad = \quad p_i \times \left( p_i^{\beta_i - \alpha_i - 1} \prod_{j\neq i} p_j^{\beta_j} \right)$$

Donc $p_i \mid \prod_{j\neq i} p_j^{\alpha_j}$. Comme au premier point, cela entraine qu'il existe $j \neq i$ tel que $p_i \mid p_j$. Comme $p_i, p_j$ sont premiers, on a $p_i = p_j$. Or, c'est impossible puisque $j \neq i$. Contradiction. Donc pour tout $i$, on a $\alpha_i = \beta_i$. Finalement, $r = s$ et pour tout $i \in [\![1, r]\!]$, on a $p_i = q_i$ et $\alpha_i = \beta_i$. Les deux décompositions sont donc bien égales. □

**Exemple 16.** La décomposition de 24 est ...

**Exemple 17.** Décomposer 630 en produits de facteurs premiers.

**Corollaire 16.32**

Il existe une infinité de nombres premiers.

*Démonstration.* On construit une infinité de nombres premiers par récurrence. On pose d'abord $p_1 = 2$, qui est premier. Ensuite, étant donné $n$ nombres premiers $p_1, p_2, \cdots, p_n$ (avec $n \geq 1$), on pose

$$N := \prod_{i=1}^{n} p_i + 1$$

Soit $i \in [\![1, n]\!]$. Comme

$$N \times 1 - p_i \times \prod_{j\neq i} p_i = 1$$

par le théorème de Bézout, on en déduit que $N \wedge p_i = 1$. Par arbitraire sur $i$, aucun des $p_i$ ne divise $N$. Or, par le lemme 16.30, $N$ admet un diviseur premier $q$. Comme $q$ divise $N$ mais que ce n'est pas le cas de $p_1, \cdots, p_n$, on a forcément que $q$ est un nombre premier qui n'est pas dans $\{p_1, \cdots, p_n\}$. On peut alors poser $p_{n+1} := q$. □

## 6.3 Valuation $p$-adique

**Définition 16.33**

Soit $p$ un nombre premier. Pour tout entier $n \in \mathbb{N}^*$, on appelle valuation $p$-adique de $n$, un nombre noté $v_p(n)$, défini comme le plus grand entier $k \in \mathbb{N}$ tel que

$$p^k \mid n \qquad \text{et} \qquad p^{k+1} \nmid n$$

Autrement dit

$$v_p(n) := \max\left\{k \in \mathbb{N} \quad | \quad p^k \mid n\right\}$$

**Exemple 18.**

- $v_2(8) = 3$ car $2^3 \mid 8$ mais $2^4 \nmid 8$.
- $v_5(100) = \ldots$
- $v_3(4) = \ldots$
- Si $p$ est un nombre premier, $v_p(p^3) = \ldots$

**Propriété 16.34**

On peut "lire" la valuation $p$-adique de $n$ sur sa décomposition en produit de facteurs premiers : si

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$$

alors pour tout $i \in [\![1, r]\!]$, $v_{p_i}(n) = \alpha_i$, et pour tout nombre premier $p \notin \{p_1, \ldots, p_r\}$, on a $v_p(n) = 0$.

**Définition 16.35 (Décomposition généralisée)**

Soit $n \in \mathbb{N}^*$. Soit $p_1 < \cdots < p_r$ des nombres premiers tels que $\{p_1, \cdots, p_r\}$ contienne tous les facteurs premiers de $n$. Il existe alors une décomposition généralisée de $n$ selon $p_1, \cdots, p_r$ :

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} \qquad \text{avec } \alpha_i \in \mathbb{N}$$

et dans ce cas, $\alpha_i = v_{p_i}(n) \in \mathbb{N}$.

Dans la décomposition généralisée, on peut donc avoir $\alpha_i = 0$. Si les nombres $p_1, \cdots, p_r$ sont fixés, cette décomposition est unique.

**Propriété 16.36**

Soit $a, b \in \mathbb{N}^*$. Alors pour tout nombre premier $p$,

1. $v_p(ab) = v_p(a) + v_p(b)$
2. $a \mid b$ si et seulement si $v_q(a) \leq v_q(b)$ pour tout nombre premier $q$.
3. Si $v_q(a) = v_q(b)$ pour tous les nombres premiers $q$, alors $a = b$.
4. $v_p(a \wedge b) = \min(v_p(a), v_p(b))$
5. $v_p(a \vee b) = \max(v_p(a), v_p(b))$

*Démonstration.* On ne prouve que les points 1 et 4. On note $p_1, \ldots, p_r$ tous les facteurs premiers qui apparaissent dans les décompositions de $a$ et $b$. Il existe alors une décomposition généralisée de $a$ et $b$ selon $p_1, \ldots, p_r$ :

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r} \qquad \alpha_i = v_{p_i}(a)$$
$$b = p_1^{\beta_1} p_2^{\beta_2} \ldots p_r^{\beta_r} \qquad \beta_i = v_{p_i}(b)$$

Alors,

$$ab = p_1^{\alpha_1+\beta_1} p_2^{\alpha_2+\beta_2} \ldots p_r^{\alpha_r+\beta_r}$$

On en déduit que pour tout $i$, $v_{p_i}(ab) = \alpha_i + \beta_i = v_{p_i}(a) + v_{p_i}(b)$. Donc l'assertion 1 est vraie.
Maintenant, si on pose $\gamma_i = \min(\alpha_i, \beta_i)$ et

$$d := p_1^{\gamma_1} p_2^{\gamma_2} \ldots p_r^{\gamma_r}$$

on va montrer que $d = a \wedge b$. Comme $\gamma_i \leq \alpha_i$, on a $d \mid a$. De même $d \mid b$. Ainsi, $d \mid (a \wedge b)$. En particulier, pour tout $i$, on a $\gamma_i \leq v_{p_i}(a \wedge b)$. Supposons par l'absurde qu'il existe $j \in [\![1, r]\!]$ tel que $\gamma_j < v_{p_j}(a \wedge b)$. Quitte à échanger $a$ et $b$, on peut par exemple supposer que $\min(\alpha_j, \beta_j) = \alpha_j$. Comme $\alpha_j + 1 \leq v_{p_j}(a \wedge b)$, on en déduit que $p_j^{\alpha_j+1} \mid (a \wedge b)$, donc que $p_j^{\alpha_j+1} \mid a$. Ainsi,

$$\alpha_j + 1 = v_{p_j}\left(p_j^{\alpha_j+1}\right) \leq v_{p_j}(a) = \alpha_j$$

Contradiction. Donc pour tout $i$, on a $v_{p_i}(d) = v_{p_i}(a \wedge b)$. On en déduit que $d = a \wedge b$. □

**Exemple 19.** Calculer le pgcd et le ppcm de 360 et 315.

### 6.4 Vérifier rapidement si un nombre est premier

Soit un entier $n \geq 2$ dont on veut savoir s'il est premier.

- Méthode longue : vérifier si pour tout $k \in [\![2, n-1]\!]$ on a bien $k \nmid n$, donc de vérifier que $\mathcal{D}(n) \cap \mathbb{N} = \{1, n\}$.
- Méthode moins longue : vérifier si pour tout nombre premier $p \leq n-1$, on a bien $p \nmid n$.
- Méthode optimale : vérifier si pour tout nombre premier $p \leq \sqrt{n}$, on a bien $p \nmid n$.

**Exemple 20.** Est-ce que 89 est un nombre premier ?

## 7 Congruences

### 7.1 Définition et relation d'équivalence

**Définition 16.37 (Congruences)**

Soit un entier $n \geq 2$ et $a, b \in \mathbb{Z}$. On dit que $a$ est congru à $b$ modulo $n$ si $n \mid (b-a)$. On note alors

$$a \equiv b \ [n]$$

Certains auteurs notent parfois $a \equiv b \pmod{n}$. Une caractérisation très utile est :

$$\boxed{a \equiv b \ [n] \iff \exists k \in \mathbb{Z} \quad a - b = kn}$$

**Remarque.** $a \equiv 0 \ [2]$ si et seulement si $a$ est pair, ou encore $a \in 2\mathbb{Z}$. De même, $a \equiv 1 \ [2] \iff a \in 2\mathbb{Z}+1$.

**Exemple 21.** $10 \equiv 3 \ [7]$ et $3 \equiv -11 \ [7]$. Pour tout $n \in \mathbb{Z}$, on a $5n+8 \equiv 3 \ [5]$.

**Exemple 22.** Résoudre l'équation $x \equiv 2 \ [7]$.

**Propriété 16.38 (Relation "congru modulo $n$")**

Soit $a, b \in \mathbb{Z}$ et un entier $n \geq 2$.

1. La relation "congru modulo $n$" est une relation d'équivalence :
   - $a \equiv a\ [n]$
   - si $a \equiv b\ [n]$, alors $b \equiv a\ [n]$.
   - si $a \equiv b\ [n]$ et $b \equiv c\ [n]$, alors $a \equiv c\ [n]$.
2. $a \equiv b\ [n]$ si et seulement si $a$ et $b$ ont le même reste quand on fait leur division euclidienne par $n$.
3. Il y a donc $n$ classes d'équivalence pour la relation "congru modulo $n$" :

$$\overline{0}, \overline{1}, \cdots, \overline{n-1}$$

(Une classe pour chaque reste possible)

## 7.2 Opérations et congruences

**Propriété 16.39 (Opérations sur les congruences)**

Soit $a, b, c, d \in \mathbb{Z}$ et un entier $n \geq 2$.

1. $a \equiv b\ [n] \quad \Longrightarrow \quad \forall k \in \mathbb{Z} \quad a + kn \equiv b\ [n]$
2. On peut additionner, soustraire ou multiplier les congruences :

$$\begin{cases} a \equiv b\ [n] \\ c \equiv d\ [n] \end{cases} \Longrightarrow \begin{cases} a + c \equiv b + d\ [n] \\ a - c \equiv b - d\ [n] \\ ac \equiv bd\ [n] \end{cases}$$

3. En particulier, pour tout $k \in \mathbb{Z}$

$$a \equiv b\ [n] \quad \Longrightarrow \quad ka \equiv kb\ [n]$$

4. On peut passer à la puissance dans une congruence : pour tout $k \in \mathbb{N}$,

$$a \equiv b\ [n] \Longrightarrow a^k \equiv b^k\ [n]$$

*Démonstration.* On ne montre que le deuxième point. On suppose que $n \mid (b-a)$ et $n \mid (d-c)$. Donc,

$$\begin{array}{lll} n \mid (b-a+d-c) & n \mid [b-a-(d-c)] & n \mid [(b-a)d + a(d-c)] \\ \Longrightarrow n \mid [b+d-(a+c)] & \Longrightarrow n \mid [b-d-(a-c)] & \Longrightarrow n \mid (bd-ac) \\ \Longrightarrow a+c \equiv b+d\ [n] & \Longrightarrow a-c \equiv b-d\ [n] & \Longrightarrow ac \equiv bd\ [n] \end{array}$$

□

**Exemple 23.** Montrer que $9^{2023} \equiv -1\ [10]$.

**Exemple 24.** Calculer le reste de la division euclidienne de $7^{129}$ par 48.

## 7.3 La division et la congruence

***Attention*** la division dans une congruence n'est pas autorisée en général :

$$9 \equiv 3\ [6] \qquad \text{mais} \qquad \frac{9}{3} \not\equiv \frac{3}{3}\ [6]$$

Par contre, si $a, b, n$ sont tous divisibles par un entier $d \in \mathbb{N}^*$, alors la division est possible :

**Propriété 16.40 (Division et congruence – crochet inclus)**

Soit $x, y \in \mathbb{Z}$, $a \in \mathbb{Z}^*$ et $n \geq 2$ un entier. On a $\quad ax \equiv ay\ [an] \iff x \equiv y\ [n]$.

Par exemple $\quad 9 \equiv 3\ [6] \quad '' \implies '' \quad 3 \equiv 1\ [2]$

**Définition 16.41 (Inverse modulo $n$)**

Soit $a \in \mathbb{Z}$ et un entier $n \geq 2$. On dit que $a$ admet un inverse modulo $n$ si

$$\exists b \in \mathbb{Z} \qquad ab \equiv 1\ [n]$$

Un entier $b \in \mathbb{Z}$ qui vérifie cela est appelé UN inverse de $a$ modulo $n$.

Il n'y a pas unicité : si $b$ est un inverse de $a$ modulo $n$, les autres inverses sont les entiers $b + kn$ avec $k \in \mathbb{Z}$.

**Exemple 25.** Donner trois inverses de 5 modulo 8 :

**Propriété 16.42 (Passage à l'inverse dans une congruence)**

Soit $a \in \mathbb{Z}$ et un entier $n \geq 2$. Alors $a$ admet un inverse modulo $n$ si et seulement si $a \wedge n = 1$.
Dans ce cas, si on note $b$ cet inverse, alors

$$\forall x, c \in \mathbb{Z} \qquad ax \equiv c\ [n] \iff x \equiv bc\ [n]$$

**Corollaire 16.43 (Division et congruence – crochet exclu)**

Soit $x, y \in \mathbb{Z}$, $a \in \mathbb{Z}^*$ et $n \geq 2$ un entier. Si $\boxed{a \wedge n = 1}$, alors $\quad ax \equiv ay\ [n] \iff x \equiv y\ [n]$.

*Démonstration.* $ax \equiv ay\ [n] \iff n \mid (ax - ay) \iff n \mid a(x-y) \iff n \mid x - y$ où le sens direct de la dernière équivalence utilise le lemme de Gauss. Enfin, $n \mid x - y \iff x \equiv y\ [n]$. □

**Méthode (Trouver un inverse modulo $n$)**

Soit $a \in \mathbb{Z}$ et un entier $n \geq 2$ tels que $a \wedge n = 1$. Pour trouver un inverse de $a$ modulo $n$, il suffit de trouver un couple de coefficients de Bézout $(u, v)$ tels que

$$au + nv = 1$$

Dans ce cas, $au \equiv 1\ [n]$, donc $u$ est un inverse de $a$ modulo $n$.

**Exercice 1.** Résoudre (dans $\mathbb{Z}$) l'équation $5x \equiv 2\ [7]$.

**Méthode (Résoudre une équation sur les congruences)**

Étant donné $A, B, N \in \mathbb{Z}$, on cherche à résoudre $Ax \equiv B\ [N]$ d'inconnue $x \in \mathbb{Z}$.

1. On détermine $d := A \wedge N$.
2. Si $d$ ne divise pas $B$, il n'y a pas de solution.
   - En effet, s'il existait une solution $x \in \mathbb{Z}$, alors il existerait $k \in \mathbb{Z}$ tel que $B = Ax + kN$. Or, $d \mid A$ et $d \mid N$ donc $d \mid (Ax + kN)$, càd $d \mid B$. Contradiction.
3. Lorsque $d \mid B$ :
   (a) On pose
   $$a := \frac{A}{d} \in \mathbb{Z} \qquad b := \frac{B}{d} \in \mathbb{Z} \qquad n := \frac{N}{d} \in \mathbb{Z}$$
   et on divise la congruence (crochet inclus) par $d$ : $Ax \equiv B\ [N] \iff ax \equiv b\ [n]$.
   (b) Par construction de $a$ et $n$, nécessairement $a \wedge n = 1$. Alors on détermine un inverse de $a$ modulo $n$ : on le notera (ici) $c$.
   (c)
   $$ax \equiv b\ [n] \iff x \equiv cb\ [n] \iff \exists k \in \mathbb{Z} \quad x = cb + kn$$
   donc $\mathcal{S} = \{cb + kn \mid k \in \mathbb{Z}\}$.

## 7.4 Petit théorème de Fermat

**Lemme 16.44**

Soit $p$ un nombre premier.

$$\forall a,b\in\mathbb{Z}\qquad (a+b)^p\equiv a^p+b^p\ [p]$$

*Démonstration.* Par la formule du binôme, on a

$$(a+b)^p=a^p+b^p+\sum_{k=1}^{p-1}\binom{p}{k}a^kb^{p-k}$$

On va montrer que pour tout $k\in[\![1,p-1]\!]$, on a $p\mid\binom{p}{k}$. Si on prouve cela, alors on aura

$$p\left|\sum_{k=1}^{p-1}\binom{p}{k}a^kb^{p-k}\right.$$

et donc $(a+b)^p\equiv a^p+b^p\ [p]$.

Montrons donc que $p\mid\binom{p}{k}$. On a

$$\binom{p}{k}=\frac{p!}{k!(p-k)!}=\frac{p}{k}\frac{(p-1)!}{(k-1)!(p-k)!}=\frac{p}{k}\frac{(p-1)!}{(k-1)!((p-1)-(k-1))!}=\frac{p}{k}\binom{p-1}{k-1}$$

Ainsi, $p\binom{p-1}{k-1}=k\binom{p}{k}$ et donc $p\mid k\binom{p}{k}$. Or, comme $1\leq k\leq p-1$ et que $p$ est premier, on a $p\wedge k=1$. Par le lemme de Gauss, on en déduit que $p\mid\binom{p}{k}$. D'où le résultat. □

**Théorème 16.45 (Petit théorème de Fermat)**

Si $p$ est un nombre premier et $a\in\mathbb{Z}$, alors

$$a^p\equiv a\ [p]$$

De plus, si $a\wedge p=1$, alors

$$a^{p-1}\equiv 1\ [p]$$

*Démonstration.* Si $a^p\equiv a\ [p]$ et $a\wedge p=1$, alors on peut diviser par $a$ dans la congruence et en déduire que $a^{p-1}\equiv 1\ [p]$. Il suffit donc de montrer que $a^p\equiv a\ [p]$.

On fait d'abord la preuve pour $a\in\mathbb{N}$, par récurrence sur $a$.

- Si $a=0$, alors $0^p=0$ donc $0^p\equiv 0\ [p]$. La propriété est vraie au rang 0.
- Supposons que $a^p\equiv a\ [p]$ pour un $a\in\mathbb{N}$, et montrons que $(a+1)^p\equiv a+1\ [p]$. Par le lemme ci-dessus, comme $p$ est premier,

$$\begin{aligned}(a+1)^p&\equiv a^p+1^p\ [p]\\&\equiv a+1^p\ [p]&&\text{par hypothèse de récurrence}\\&\equiv a+1\ [p]\end{aligned}$$

  Donc la propriété est vraie au rang $a+1$.

- Finalement, pour tout $a \in \mathbb{N}$, $a^p \equiv a\ [p]$.

Faisons enfin la preuve pour $a \in \mathbb{Z} \setminus \mathbb{N}$. Comme $p \geq 2$, il existe $k \in \mathbb{N}$ (assez grand) tel que $a + kp \geq 0$. On pose alors $b := a + kp$. Par construction, $b \equiv a\ [p]$ et donc $b^p \equiv a^p\ [p]$. De plus, comme $b \geq 0$, on a montré que $b^p \equiv b\ [p]$. Ainsi,

$$a^p \equiv b^p \equiv b \equiv a\ [p]$$

□

**Exemple 26.** Quel est le reste de la division euclidienne de $14^{314}$ par 11 ?

## 8 Équations diophantiennes

**Définition 16.46 (Équation diophantienne)**

On appelle équation diophantienne une équation dont la ou les inconnues sont des entiers relatifs.

**Exemple 27.** L'équation $2x + 7y = 3$ d'inconnues $x, y \in \mathbb{Z}$.
L'équation $x^2 + y^2 = z^2$ d'inconnues $x, y, z \in \mathbb{Z}$.

La résolution de ces équations est souvent non triviale. Néanmoins, il y a un cas particulier d'équation qu'il faut savoir traiter sans indication : les équations diophantiennes du premier ordre à deux inconnues :

**Méthode (Résolution d'une équation diophantienne du type $Ax + By = C$)**

Soit $A, B, C \in \mathbb{Z}$. On cherche à résoudre l'équation $Ax + By = C$ d'inconnues $x, y \in \mathbb{Z}$.

1. On détermine $d = A \wedge B$.
2. Si $d \nmid C$, alors il n'y a pas de solution.
3. Lorsque $d \mid C$ :
   (a) On pose $a = \dfrac{A}{d}$, $b = \dfrac{B}{d}$, $c = \dfrac{C}{d}$, et alors on résoud à la place $ax + by = c$.
   (b) Par construction, $a \wedge b = 1$. On cherche alors $u, v \in \mathbb{Z}$ tels que
   $$au + bv = 1$$
   (c) En multipliant par $c$ cette équation, on obtient une solution particulière $(x_0, y_0) = (cu, cv)$.
   (d) Alors,
   $$\mathcal{S} = \{\ (x_0 - bk,\ y_0 + ak)\ \mid\ k \in \mathbb{Z}\ \}$$

*Démonstration.* Justifions le dernier point : on vérifie directement que pour tout $k \in \mathbb{Z}$, $(x_0 - bk, y_0 + ak) \in \mathcal{S}$. Montrons l'autre inclusion : soit $(x,y) \in \mathcal{S}$. Alors

$$\begin{cases} ax + by = c \\ ax_0 + by_0 = c \end{cases} \implies a(x - x_0) + b(y - y_0) = 0$$

Ainsi, $a(x-x_0) = -b(y-y_0)$ : comme $a \wedge (-b) = a \wedge b = 1$, par le lemme de Gauss, $a \mid (y - y_0)$, donc il existe $k \in \mathbb{Z}$ tel que $\boxed{y = y_0 + ak}$. Alors,

$$x - x_0 = -\frac{1}{a} b(y - y_0) = -bk$$

d'où $\boxed{x = x_0 - bk}$. □

Attention, dans la preuve ci-dessus, il faut bien prendre le même $k$ ! On peut montrer que $b \mid (x - x_0)$ indépendamment mais cela mène à :

$$\exists k' \in \mathbb{Z} \qquad x = x_0 + bk'$$

et a priori on ne saurait justifier que $k' = -k$.

**Remarque.** Il faut savoir refaire la démonstration ci-dessus.