# Arithmétique dans Z

## I. Divisibilité dans l'anneau des entiers

Ce chapitre construit l'arithmétique des entiers relatifs à partir d'un seul outil : la division euclidienne. Tous les résultats seront donc démontrés. On note $\mathbb{Z}$ l'ensemble des entiers relatifs et $\mathbb{N}$ celui des entiers naturels. On admet que toute partie non vide de $\mathbb{N}$ possède un plus petit élément. Cette propriété fondamentale de $\mathbb{N}$ sert dans presque toutes les preuves.

**Définition :**

Soient $a$ et $b$ deux entiers relatifs. On dit que $b$ **divise** $a$, et on note $b \mid a$, s'il existe $k \in \mathbb{Z}$ tel que $a = kb$. On dit aussi que $a$ est un **multiple** de $b$, ou que $b$ est un **diviseur** de $a$. L'ensemble des multiples de $b$ se note $b\mathbb{Z}$.

Ainsi, $0$ est multiple de tout entier, tandis que $0$ ne divise que lui-même. De plus, $1$ et $-1$ divisent tous les entiers. Enfin, $b$ et $-b$ ont exactement les mêmes multiples et les mêmes diviseurs.

**Propriété :**

Soient $a, b, c$ des entiers relatifs.

- Réflexivité : $a \mid a$. Transitivité : si $a \mid b$ et $b \mid c$, alors $a \mid c$.
- Si $a \mid b$ et $b \mid a$, alors $|a| = |b|$.

Téléchargé depuis https://mathovore.fr - Mathovore site de maths.

- Si $d \mid a$ et $d \mid b$, alors $d \mid au + bv$ pour tous $u, v \in \mathbb{Z}$.
- Si $b \mid a$ et $a \neq 0$, alors $|b| \leq |a|$.

**Démonstration :**

Montrons d'abord la combinaison linéaire. Si $a = kd$ et $b = \ell d$, alors $au + bv = (ku + \ell v)d$, donc $d$ divise $au + bv$. Ensuite, si $a = kb$ avec $a \neq 0$, alors $k \neq 0$, donc $|k| \geq 1$ et $|a| = |k|\,|b| \geq |b|$. Enfin, si $a \mid b$ et $b \mid a$, deux cas se présentent. Si $a = 0$, alors $b$ est multiple de $0$, donc $b = 0$. Sinon $b \neq 0$ aussi, et l'inégalité précédente donne $|a| \leq |b| \leq |a|$. La transitivité se prouve de la même façon.

**Exemple :**

Cherchons les entiers $n$ tels que $n + 2$ divise $3n + 11$. Comme $n + 2$ divise $3(n+2)$, il divise la différence $3n + 11 - 3(n + 2) = 5$. Par conséquent $n + 2 \in \{-5, -1, 1, 5\}$, autrement dit $n \in \{-7, -3, -1, 3\}$. Réciproquement, chacune de ces valeurs convient.

## II. La division euclidienne dans Z

La division euclidienne est le théorème de départ de toute l'arithmétique. En effet, elle permet de comparer un entier quelconque aux multiples d'un entier fixé.

**Théorème :**

Soient $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$. Il existe un **unique** couple $(q, r) \in \mathbb{Z}^2$ tel que

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

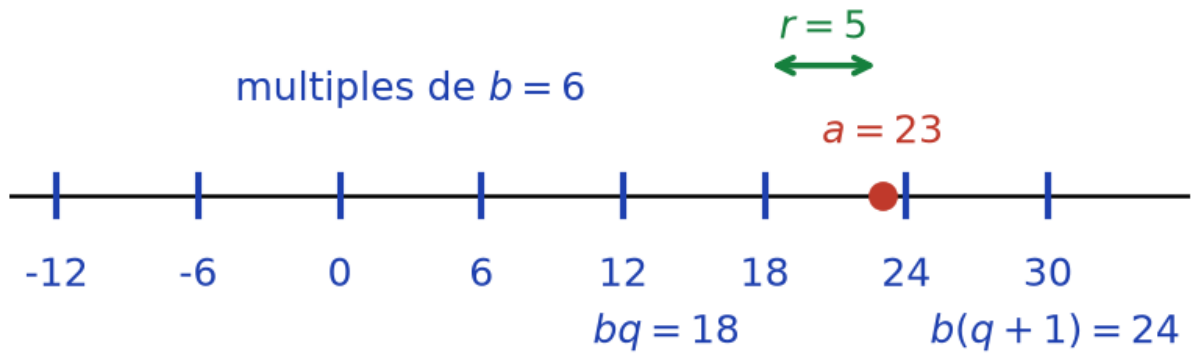
L'entier $q$ est le **quotient** et $r$ le **reste** de la division euclidienne de $a$ par $b$.

**Démonstration :**

Existence. Considérons l'ensemble $E = \{a, bk \mid k \in \mathbb{Z}\} \cap \mathbb{N}$. Il est non vide : pour $k = -|a|$, on a $a + b|a| \geq a + |a| \geq 0$. Il possède donc un plus petit élément $r = a - bq$. Par construction $r \geq 0$. De plus, $r - b = a - b(q+1)$ est strictement plus petit que $r$, donc il n'appartient pas à $E$. Ainsi $r - b < 0$, c'est-à-dire $r < b$.

Unicité. Supposons $a = bq + r = bq' + r'$ avec $0 \leq r, r' < b$. Alors $b(q - q') = r' - r$, et $|r' - r| < b$. Donc $b$ divise un entier de valeur absolue strictement inférieure à $b$. D'après la propriété précédente, cet entier est nul. Par conséquent $r = r'$, puis $q = q'$.

Concrètement, $bq$ est le plus grand multiple de $b$ inférieur ou égal à $a$. Comme le montre la figure ci-dessous, l'entier $a = 23$ se situe entre les multiples consécutifs $18$ et $24$ de $b = 6$ : le reste $r = 5$ mesure l'écart entre $a$ et $bq$.




**Exemple :**

Téléchargé depuis https://mathovore.fr - Mathovore site de maths.

Pour $a = -23$ et $b = 6$, on écrit $-23 = 6 \times (-4) + 1$. Le quotient vaut donc $-4$ et le reste $1$. Attention, l'écriture $-23 = 6 \times (-3) - 5$ ne convient pas, car le reste doit être positif.

**Corollaire :**

Pour $b \geq 1$, l'entier $b$ divise $a$ si et seulement si le reste de la division euclidienne de $a$ par $b$ est nul. De plus, tout entier s'écrit d'une unique façon $bq + r$ avec $r \in \{0, 1, \ldots, b-1\}$.

Ce corollaire justifie les raisonnements « par disjonction des restes ». Par exemple, tout entier est de la forme $2k$ ou $2k+1$. De même, tout entier est de la forme $3k$, $3k+1$ ou $3k+2$.

# III. PGCD et algorithme d'Euclide

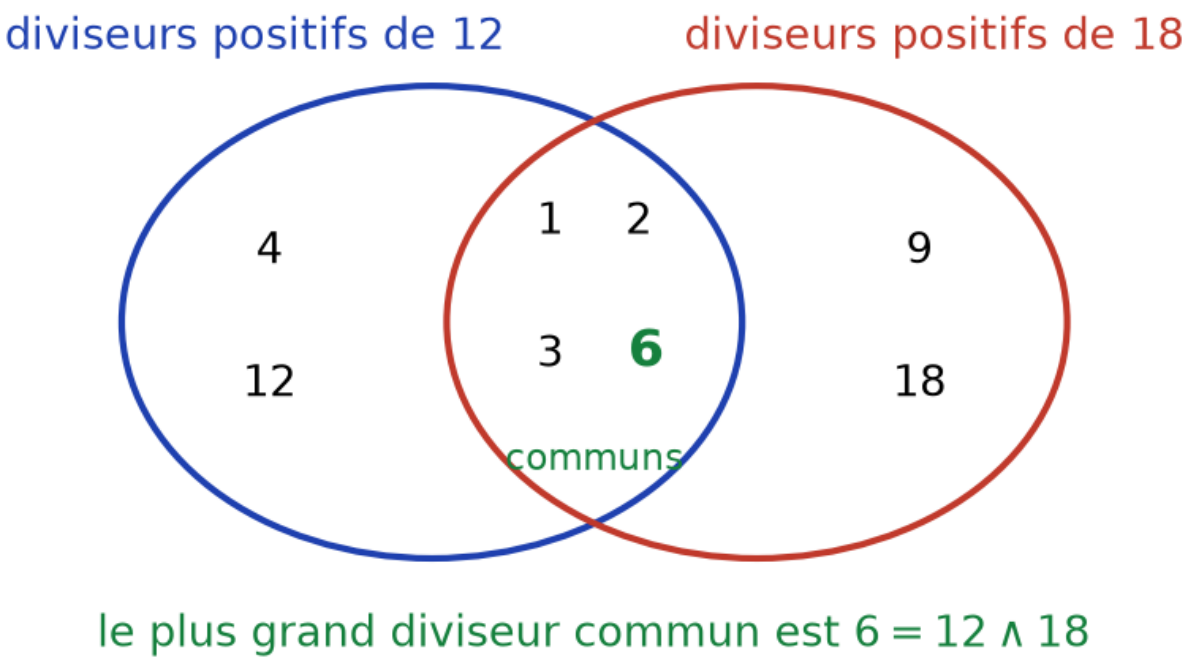
## 1. Définition du PGCD

Soient $a$ et $b$ deux entiers non tous deux nuls. Leurs diviseurs communs sont en nombre fini, car ils sont majorés en valeur absolue par $\max(|a|, |b|)$. De plus, $1$ en fait partie. Il existe donc un plus grand diviseur commun.

**Définition :**

Le **PGCD** de deux entiers $a$ et $b$ non tous deux nuls est le plus grand entier naturel qui divise à la fois $a$ et $b$. On le note $a \wedge b$ ou $\text{pgcd}(a, b)$. Par convention, $0 \wedge 0 = 0$. On dit que $a$ et $b$ sont **premiers entre eux** lorsque $a \wedge b = 1$.

Le diagramme de Venn ci-dessous représente les diviseurs positifs de $12$ et de $18$. Leur intersection contient $1$, $2$, $3$ et $6$ ; le plus grand de ces diviseurs communs est $6$.




Remarquons que $a \wedge b = |a| \wedge |b|$ et que $a \wedge 0 = |a|$. On peut donc se ramener à des entiers naturels.

## 2. Le lemme clé et l'algorithme d'Euclide

**Lemme :**

Soient $a, b, q$ trois entiers. Alors les couples $(a, b)$ et $(b, a - bq)$ ont les mêmes diviseurs communs. En particulier, si $r$ est le reste de la division de $a$ par $b \geq 1$, alors $a \wedge b = b \wedge r$.

**Démonstration :**

Posons $r = a - bq$. Si $d$ divise $a$ et $b$, alors $d$ divise la combinaison $a - bq = r$. Réciproquement, si $d$ divise $b$ et $r$, alors $d$ divise $bq + r = a$. Les deux ensembles de diviseurs communs coïncident, donc leurs plus grands éléments aussi.

Téléchargé depuis https://mathovore.fr - Mathovore site de maths.

On en déduit l'algorithme d'Euclide. On part de $r_0 = a$ et $r_1 = b$, avec $a \geq b \geq 1$. Tant que $r_k \neq 0$, on note $r_{k+1}$ le reste de la division de $r_{k-1}$ par $r_k$. Les restes forment une suite d'entiers naturels strictement décroissante. Par conséquent, elle atteint $0$ en un nombre fini d'étapes. D'après le lemme, le PGCD se conserve à chaque étape : $a \wedge b = r_n \wedge 0 = r_n$.

**Méthode :**

Pour **calculer un PGCD par l'algorithme d'Euclide**, on effectue des divisions euclidiennes successives : on divise $a$ par $b$, puis $b$ par le reste, et ainsi de suite. Le PGCD est le **dernier reste non nul**. On présente les calculs ligne par ligne, afin de pouvoir remonter ensuite l'algorithme.

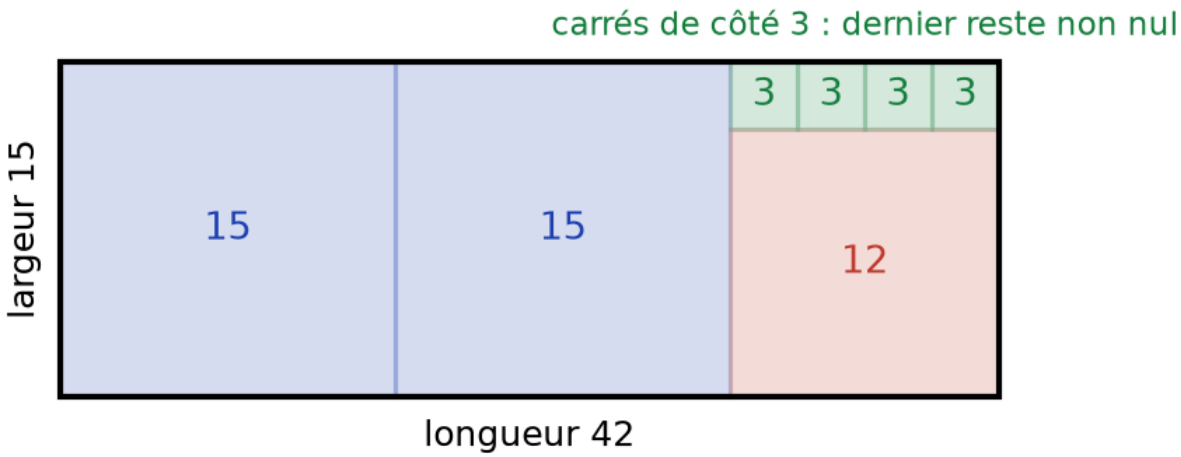
**Exemple :**

Calculons $42 \wedge 15$. On écrit successivement :

$$\begin{aligned} 42 &= 2 \times 15 + 12 \\ 15 &= 1 \times 12 + 3 \\ 12 &= 4 \times 3 + 0. \end{aligned}$$

Le dernier reste non nul vaut $3$, donc $42 \wedge 15 = 3$.

L'algorithme admet une interprétation géométrique. On découpe un rectangle de $42$ sur $15$ en carrés les plus grands possible, puis on recommence dans le rectangle restant. Comme le montre la figure ci-dessous, le dernier carré utilisé a pour côté le PGCD.




# IV. Théorème de Bézout, lemme de Gauss et PPCM

## 1. L'identité de Bézout

**Théorème :**

(Identité de Bézout.) Soient $a$ et $b$ deux entiers et $d = a \wedge b$. Il existe des entiers $u$ et $v$ tels que $au + bv = d$. De plus, l'ensemble $a\mathbb{Z} + b\mathbb{Z} = \{au + b,| u, v \in [\mamathbb?]\mathbb{Z}\}$ est exactement $d\mathbb{Z}$.

**Démonstration :**

Le cas $a = b = 0$ est immédiat. Sinon, l'ensemble $I = a\mathbb{Z} + b\mathbb{Z}$ contient un entier strictement positif, par exemple $a^2 + b^2$. Soit $\delta$ le plus petit élément strictement positif de $I$, écrit $\delta = au_0 + bv_0$. Divisons $a$ par $\delta$ : $a = \delta q + r$ avec $0 \leq r < \delta$. Alors $r = a(1 - qu_0) + b(-qv_0)$ appartient à $I$. Par minimalité de $\delta$, on obtient $r = 0$, donc $\delta \mid a$. De même, $\delta \mid b$, donc $\delta \leq d$.

D'autre part, $d$ divise $a$ et $b$, donc il divise $au_0 + bv_0 = \delta$. Ainsi $d \leq \delta$, puis $\delta = d$. Enfin, tout élément de $I$ est multiple de $d$, et tout multiple $kd = a(ku_0) + b(kv_0)$ est dans

Téléchargé depuis https://mathovore.fr - Mathovore site de maths.

$I$. Donc $I = d\mathbb{Z}$.

**Corollaire :**

Un entier $d \geq 0$ divisant $a$ et $b$ est égal à $a \wedge b$ si et seulement s'il existe $u, v$ tels que $au + bv = d$. De plus, tout diviseur commun de $a$ et $b$ divise $a \wedge b$. Enfin, pour $k \in \mathbb{N}$, on a $(ka) \wedge (kb) = k(a \wedge b)$.

**Théorème :**

(**Théorème de Bézout**.) Les entiers $a$ et $b$ sont premiers entre eux si et seulement s'il existe $u, v \in \mathbb{Z}$ tels que $au + bv = 1$.

**Démonstration :**

Le sens direct découle de l'identité de Bézout avec $d = 1$. Réciproquement, si $au + bv = 1$, tout diviseur commun positif de $a$ et $b$ divise $1$, donc vaut $1$. Ainsi $a \wedge b = 1$.

## 2. Déterminer des coefficients de Bézout

**Méthode :**

Pour **déterminer des coefficients de Bézout**, on remonte l'algorithme d'Euclide. On isole le dernier reste non nul dans l'avant-dernière division. Ensuite, on remplace chaque reste par son expression tirée de la division précédente. À la fin, on vérifie toujours l'égalité obtenue par un calcul direct.

**Exemple :**

Reprenons $42 \wedge 15 = 3$. D'abord $3 = 15 - 12$. Ensuite $12 = 42 - 2 \times 15$. Par conséquent $3 = 15 - (42 - 2 \times 15) = 3 \times 15 - 42$. On obtient $u = -1$ et $v = 3$, et l'on vérifie : $-42 + 45 = 3$.

## 3. Le lemme de Gauss

**Théorème :**

(**Lemme de Gauss**.) Soient $a, b, c$ trois entiers. Si $a$ divise $bc$ et si $a \wedge b = 1$, alors $a$ divise $c$.

**Démonstration :**

D'après le théorème de Bézout, il existe $u, v$ tels que $au + bv = 1$. En multipliant par $c$, on obtient $c = acu + bcv$. Or $a$ divise $acu$, et $a$ divise $bcv$ puisqu'il divise $bc$. Par conséquent $a$ divise leur somme $c$.

**Corollaire :**

Si $a \mid c$, $b \mid c$ et $a \wedge b = 1$, alors $ab \mid c$. De plus, si $a$ est premier avec $b$ et avec $c$, alors $a$ est premier avec $bc$.

**Démonstration :**

Téléchargé depuis https://mathovore.fr - Mathovore site de maths.

Écrivons $c = ak$. Alors $b$ divise $ak$ et $b \wedge a = 1$, donc $b \mid k$ par le lemme de Gauss. Ainsi $k = b\ell$ et $c = ab\ell$. Pour le second point, on multiplie deux relations $au + bv = 1$ et $au' + cw = 1$. On obtient $a(\ldots) + bc\,vw = 1$, ce qui conclut par le théorème de Bézout.

## 4. Le PPCM

**Définition :**

Soient $a$ et $b$ deux entiers non nuls. Le **PPCM** de $a$ et $b$, noté $a \vee b$, est le plus petit entier strictement positif multiple à la fois de $a$ et de $b$.

**Proposition :**

Pour $a, b \in \mathbb{N}^*$, on a $(a \wedge b) \times (a \vee b) = ab$. De plus, les multiples communs de $a$ et $b$ sont exactement les multiples de $a \vee b$.

**Démonstration :**

Posons $d = a \wedge b$, $a = da'$ et $b = db'$. Alors $a' \wedge b' = 1$, car $d(a' \wedge b') = a \wedge b = d$. Soit $m$ un multiple commun de $a$ et $b$. On écrit $m = da'k$. Comme $db'$ divise $da'k$, on obtient $b' \mid a'k$, puis $b' \mid k$ par le lemme de Gauss. Ainsi $m$ est multiple de $da'b'$. Réciproquement, $da'b'$ est un multiple commun. Donc $a \vee b = da'b'$, et $d \times da'b' = ab$.

## 5. Équations diophantiennes linéaires

On cherche les couples d'entiers $(x, y)$ tels que $ax + by = c$, où $a$ et $b$ sont non nuls. Géométriquement, ce sont les points à coordonnées entières d'une droite du plan.

## Théorème :

Soit $d = a \wedge b$. L'équation $ax + by = c$ a des solutions entières si et seulement si $d \mid c$. Dans ce cas, on pose $a = da'$, $b = db'$, et l'on fixe une solution particulière $(x_0, y_0)$. Les solutions sont alors exactement les couples

$$(x, y) = (x_0 + kb', \\ ,y_0 - ka'), \ k \in \mathbb{Z}.$$

## Démonstration :

La condition $d \mid c$ est nécessaire, car $d$ divise $ax + by$. Elle est suffisante : si $c = dc'$ et $au + bv = d$, alors $(uc', vc')$ est solution. Soit ensuite $(x, y)$ une solution. Par différence, $a(x - x_0) = -b(y - y_0)$, puis, en divisant par $d$, $a'(x - x_0) = -b'(y - y_0)$. Ainsi $b'$ divise $a'(x - x_0)$, avec $a' \wedge b' = 1$. Le lemme de Gauss donne $x - x_0 = kb'$, puis $y - y_0 = -ka'$. Réciproquement, ces couples sont bien solutions.

## Méthode :

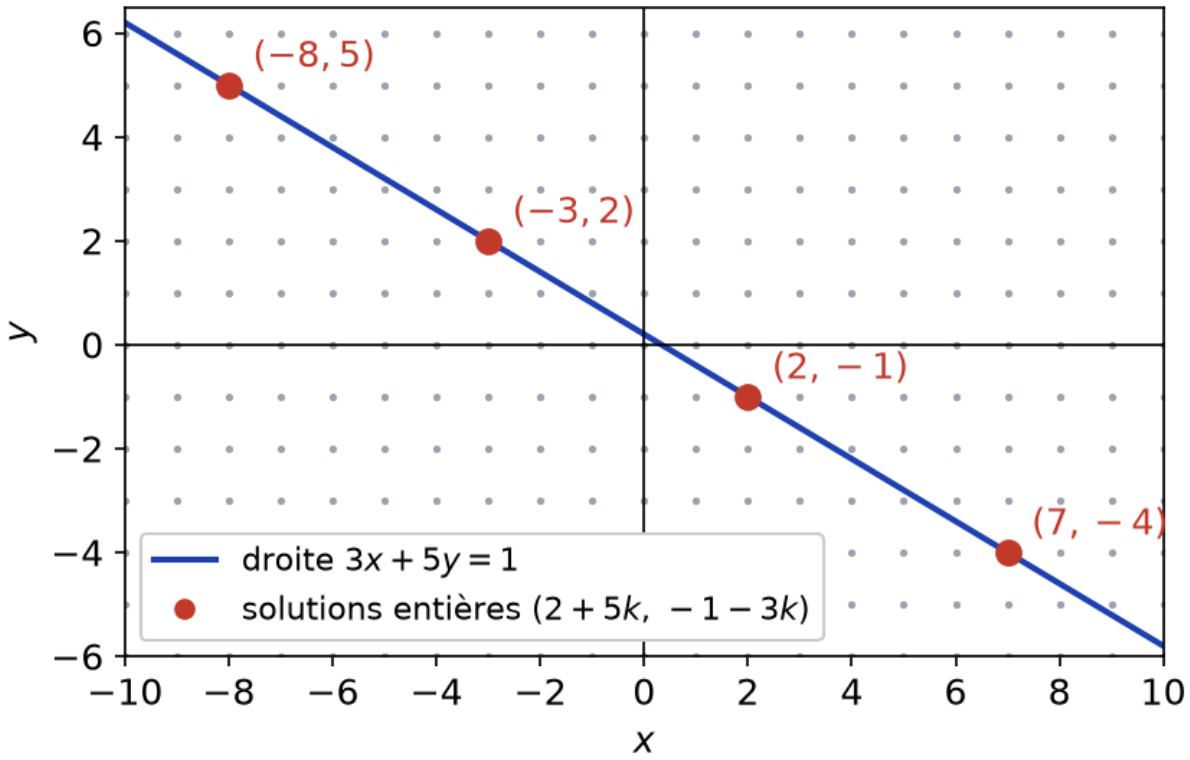
Pour **résoudre une équation diophantienne** $ax + by = c$ : on calcule $d = a \wedge b$ et l'on vérifie que $d \mid c$ ; on divise l'équation par $d$ ; on trouve une solution particulière, à vue ou par l'algorithme d'Euclide remonté ; enfin, on soustrait et on applique le lemme de Gauss.

## Exemple :

Résolvons $3x + 5y = 1$. On voit que $(2, -1)$ est solution, car $6 - 5 = 1$. Les solutions sont donc les couples $(2 + 5k, -1 - 3k)$, avec $k \in \mathbb{Z}$.

Téléchargé depuis https://mathovore.fr - Mathovore site de maths.

Comme le montre la figure ci-dessous, ces solutions sont régulièrement espacées sur la droite d'équation $3x + 5y = 1$. On passe de l'une à la suivante par le vecteur $(5, -3)$.




## V. Nombres premiers et décomposition en facteurs premiers

### 1. Nombres premiers

**Définition :**

Un entier naturel $p$ est **premier** s'il est supérieur ou égal à $2$ et si ses seuls diviseurs positifs sont $1$ et $p$. Un entier $n \geq 2$ non premier est dit composé.

**Proposition :**

Tout entier $n \geq 2$ admet un diviseur premier : son plus petit diviseur $p \geq 2$. Si $n$ est composé, ce diviseur vérifie de plus $p^2 \leq n$.

**Démonstration :**

L'ensemble des diviseurs de $n$ supérieurs ou égaux à $2$ contient $n$. Il a donc un plus petit élément $p$. Si $p$ avait un diviseur $q$ avec $1 < q < p$, alors $q$ diviserait $n$, ce qui contredirait la minimalité. Donc $p$ est premier. Si $n$ est composé, alors $n = pm$ avec $m \geq 2$ diviseur de $n$. Par minimalité, $m \geq p$, donc $n \geq p^2$.

Pour tester si $n$ est premier, il suffit donc de chercher un diviseur premier $p$ avec $p^2 \leq n$. Le crible d'Ératosthène repose sur cette idée. On barre successivement les multiples de $2$, $3$, $5$ et $7$, car $11^2 > 100$. La figure ci-dessous montre le résultat pour les entiers de $1$ à $100$.

Téléchargé depuis https://mathovore.fr - Mathovore site de maths.

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 1 | **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 |

en rouge : les 25 nombres premiers inférieurs à 100

**Théorème :**

(**Euclide**.) Il existe une infinité de nombres premiers.

**Démonstration :**

Supposons qu'il n'y en ait qu'un nombre fini, $p_1, \cdots, p_k$. Posons $N = p_1 p_2 \cdots p_k + 1 \geq 3$. D'après la proposition, $N$ admet un diviseur premier $p$, qui est l'un des $p_i$. Alors $p$ divise $N$ et $p_1 \cdots p_k$, donc il divise leur différence $1$. C'est absurde, car $p \geq 2$.

**Lemme :**

(**Lemme d'Euclide**.) Soit $p$ premier. Pour tout entier $a$, soit $p \mid a$, soit $p \wedge a = 1$. Par conséquent, si $p$ divise un produit $ab$, alors $p$ divise $a$ ou $p$ divise $b$.

**Démonstration :**

Le PGCD $p \wedge a$ est un diviseur positif de $p$, donc il vaut $1$ ou $p$. S'il vaut $p$, alors $p \mid a$. Supposons maintenant $p \mid ab$ et $p \,[\nmid?]\, a$. Alors $p \wedge a = 1$, et le lemme de Gauss donne $p \mid b$. Par récurrence, si $p$ divise un produit de plusieurs facteurs, il divise l'un d'eux.

## 2. Décomposition en facteurs premiers

**Théorème :**

(**Théorème fondamental de l'arithmétique**.) Tout entier $n \geq 2$ s'écrit comme produit de nombres premiers :

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}, \; p_1 < p_2 < \ldots < p_r \text{ premiers}, \; \alpha_i \geq 1.$$

Cette écriture est unique.

Téléchargé depuis https://mathovore.fr - Mathovore site de maths.

**Démonstration :**

Existence, par récurrence forte sur $n$. Si $n$ est premier, c'est fini. Sinon, $n = ab$ avec $2 \leq a, b < n$, et l'on multiplie les décompositions de $a$ et de $b$.

Unicité, par récurrence forte également. Supposons $n = p_1 \cdots p_s = q_1 \cdots q_t$, avec des facteurs premiers répétés éventuellement. Le premier $p_1$ divise le produit des $q_j$. D'après le lemme d'Euclide, il divise l'un d'eux, disons $q_j$. Comme $q_j$ est premier, $p_1 = q_j$. On simplifie par $p_1$ et on applique l'hypothèse de récurrence à $n \,/\, p_1 < n$.

**Notation :**

Pour $p$ premier et $n \neq 0$, on note $v_p(n)$ l'exposant de $p$ dans la décomposition de $|n|$ : c'est la **valuation $p$-adique** de $n$. Elle vaut $0$ si $p \,[\nmid?]\, n$, et $v_p(ab) = v_p(a) + v_p(b)$.

**Proposition :**

Soient $a, b \geq 1$. Alors $a \mid b$ si et seulement si $v_p(a) \leq v_p(b)$ pour tout $p$ premier. De plus :

$$a \wedge b = \prod_p p^{\min(v_p(a),\, v_p(b))}, \quad a \vee b = \prod_p p^{\max(v_p(a),\, v_p(b))}.$$

**Exemple :**

On a $360 = 2^3 \times 3^2 \times 5$ et $84 = 2^2 \times 3 \times 7$. Ainsi $360 \wedge 84 = 2^2 \times 3 = 12$ et $360 \vee 84 = 2^3 \times 3^2 \times 5 \times 7 = 2520$. On retrouve bien $12 \times 2520 = 30240 = 360 \times 84$.

Pour **utiliser la décomposition en facteurs premiers**, on raisonne exposant par exposant. Par exemple, $n$ a exactement $(\alpha_1+1)\ldots(\alpha_r+1)$ diviseurs positifs. En effet, un diviseur s'écrit $p_1^{\beta_1}\ldots p_r^{\beta_r}$ avec $0 \leq \beta_i \leq \alpha_i$.

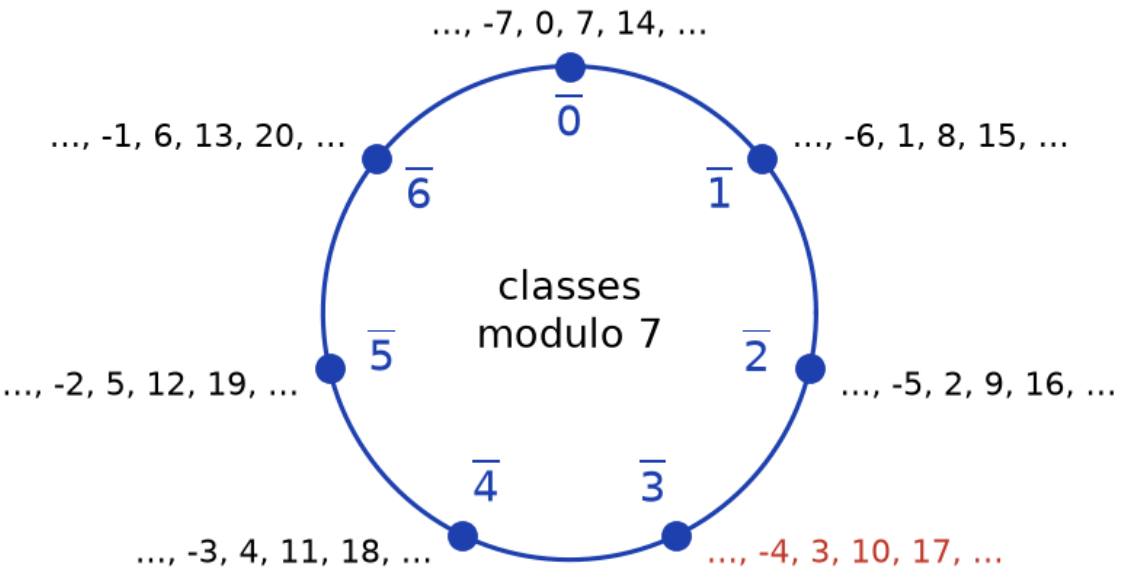
# VI. Congruences modulo n et petit théorème de Fermat

## 1. Définition et compatibilité

**Définition :**

Soit $n \geq 1$. Deux entiers $a$ et $b$ sont **congrus modulo** $n$ si $n$ divise $a-b$. On note $a \equiv b \ [n]$. Autrement dit, $a$ et $b$ ont le même reste dans la division euclidienne par $n$.

La congruence modulo $n$ est réflexive, symétrique et transitive. Elle répartit donc $\mathbb{Z}$ en $n$ classes, notées $\bar{0}, \bar{1}, \ldots, \overline{n-1}$. Comme le montre la figure ci-dessous pour $n=7$, chaque classe regroupe les entiers qui ont le même reste. Par exemple, $-4$, $3$, $10$ et $17$ sont dans la classe $\bar{3}$.




Téléchargé depuis https://mathovore.fr - Mathovore site de maths.

**Propriété :**

Si $a \underset{[n]}{\equiv} b$ et $c \underset{[n]}{\equiv} d$, alors $a + c \underset{[n]}{\equiv} b + d$ et $ac \underset{[n]}{\equiv} bd$. En particulier, $a^k \underset{[n]}{\equiv} b^k$ pour tout $k \in \mathbb{N}$.

**Démonstration :**

La somme découle de $(a + c) - (b + d) = (a - b) + (c - d)$. Pour le produit, on écrit $ac - bd = a(c - d) + d(a - b)$, qui est une combinaison de multiples de $n$. La puissance s'obtient par récurrence sur $k$.

**Attention :**

On ne peut pas simplifier librement une congruence. Par exemple, $2 \times 3 \underset{[10]}{\equiv} 2 \times 8$, mais $3 \underset{[10]}{\not\equiv} 8$. En revanche, si $ac \underset{[n]}{\equiv} bc$ et $c \wedge n = 1$, alors $a \underset{[n]}{\equiv} b$ d'après le lemme de Gauss.

**Proposition :**

L'entier $a$ possède un **inverse modulo** $n$, c'est-à-dire un entier $u$ tel que $au \underset{[n]}{\equiv} 1$, si et seulement si $a \wedge n = 1$. Dans ce cas, l'équation $ax \underset{[n]}{\equiv} c$ équivaut à $x \underset{[n]}{\equiv} uc$.

**Démonstration :**

Dire que $au \underset{[n]}{\equiv} 1$ revient à dire qu'il existe $v$ tel que $au + nv = 1$. D'après le théorème de

Bézout, cela équivaut à $a \wedge n = 1$. Ensuite, on multiplie $ax \equiv c$ par $u$ pour obtenir $x \equiv uc$, et inversement par $a$.

## 2. Calculer avec des congruences

**Méthode :**

Pour **calculer le reste de $a^k$ modulo $n$**, on remplace d'abord $a$ par un représentant petit, éventuellement négatif. Ensuite, on cherche une puissance $a^m \equiv 1$ ou $a^m \equiv -1$. On écrit enfin la division euclidienne $k = mq + r$, ce qui donne $a^k \equiv (a^m)^q a^r$.

**Exemple :**

Cherchons le reste de $5^{2026}$ modulo $13$. On a $5^2 = 25 \underset{[13]}{\equiv} -1$, donc $5^4 \underset{[13]}{\equiv} 1$. Or $2026 = 4 \times 506 + 2$. Ainsi $5^{2026} \underset{[13]}{\equiv} 5^2 \equiv -1 \equiv 12$. Le reste vaut donc $12$.

De même, les critères de divisibilité se démontrent par congruences. Comme $10 \underset{[9]}{\equiv} 1$, tout entier est congru à la somme de ses chiffres modulo $9$. De plus, $10 \underset{[11]}{\equiv} -1$ fournit le critère de divisibilité par $11$.

## 3. Le petit théorème de Fermat

**Lemme :**

Si $p$ est premier et $1 \leq k \leq p-1$, alors $p$ divise $\binom{p}{k}$.

Téléchargé depuis https://mathovore.fr - Mathovore site de maths.

**Démonstration :**

La formule du capitaine donne $k\binom{p}{k} = p\,[\backslash\mathrm{let?}](\binom{p-1}{k-1}[\backslash\mathrm{righht?}])$ . Ainsi $p$ divise $k\binom{p}{k}$ . Or $p \wedge k = 1$ , car $1 \leq k < p$ . Le lemme de Gauss conclut.

**Théorème :**

(**Petit théorème de Fermat**.) Soit $p$ un nombre premier. Pour tout $a \in \mathbb{Z}$ , on a $a^p \underset{[p]}{\equiv} a$ . Si de plus $p\,[\backslash\mathrm{nmid?}]\,a$ , alors $a^{p-1} \underset{[p]}{\equiv} 1$ .

**Démonstration :**

Montrons d'abord le résultat pour $a \in \mathbb{N}$ , par récurrence. Il est clair pour $a = 0$ . Supposons $a^p \underset{[p]}{\equiv} a$ . La formule du binôme et le lemme donnent $(a+1)^p \underset{[p]}{\equiv} a^p + 1$ , car les termes intermédiaires sont multiples de $p$ . Donc $(a+1)^p \underset{[p]}{\equiv} a+1$ .

Pour $a < 0$ , on se ramène à un entier naturel $a + mp$ , congru à $a$ . Enfin, si $p\,[\backslash\mathrm{nmid?}]\,a$ , alors $p$ divise $a(a^{p-1} - 1)$ et $p \wedge a = 1$ . Le lemme de Gauss donne $p \mid a^{p-1} - 1$ .

**Exemple :**

Calculons le reste de $2^{100}$ modulo $11$ . Le petit théorème de Fermat donne $2^{10} \underset{[11]}{\equiv} 1$ . Or $100 = 10 \times 10$ , donc $2^{100} \underset{[11]}{\equiv} 1$ . Le reste vaut $1$ .

**Remarque :**

La réciproque est fausse. Par exemple, $341 = 11 \times 31$ n'est pas premier, et pourtant $2^{340} \equiv 1 \ [341]$. Le théorème de Fermat sert donc surtout à prouver qu'un nombre est composé, et à calculer des puissances.

## Ce qu'il faut retenir

- Tout repose sur la **division euclidienne** : $a = bq + r$ avec $0 \leq r < b$, de façon unique.
- Si $d$ divise $a$ et $b$, alors $d$ divise toute combinaison $au + bv$.
- L'**algorithme d'Euclide** repose sur $a \wedge b = b \wedge r$ : le PGCD est le dernier reste non nul.
- L'**identité de Bézout** : $a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\mathbb{Z}$ ; on trouve $u, v$ en remontant l'algorithme.
- Le **lemme de Gauss** : si $a \mid bc$ et $a \wedge b = 1$, alors $a \mid c$.
- $(a \wedge b)(a \vee b) = ab$ pour des entiers naturels non nuls.
- L'équation $ax + by = c$ a des solutions si et seulement si $a \wedge b$ divise $c$ ; elles forment une famille $(x_0 + kb', y_0 - ka')$.
- Il existe une infinité de nombres premiers, et la **décomposition en facteurs premiers** est unique.
- Les congruences modulo $n$ sont compatibles avec la somme et le produit ; $a$ est inversible modulo $n$ si et seulement si $a \wedge n = 1$.
- **Petit théorème de Fermat** : $a^p \equiv a \ [p]$, et $a^{p-1} \equiv 1 \ [p]$ si $p \ [\nmid?] \ a$.

## Questions fréquentes sur arithmétique dans Z

Téléchargé depuis https://mathovore.fr - Mathovore site de maths.

Quelle différence entre le théorème de Bézout et l'identité de Bézout ?

L'identité de Bézout affirme que pour tous entiers $a$ et $b$, il existe $u, v$ tels que $au + bv = a \wedge b$. Le théorème de Bézout en est le cas particulier caractéristique : $a \wedge b = 1$ si et seulement s'il existe $u, v$ tels que $au + bv = 1$. Attention, une relation $au + bv = d$ avec $d > 1$ ne prouve pas que $d$ est le PGCD.

Comment trouver des coefficients de Bézout sans se tromper ?

On écrit l'algorithme d'Euclide ligne par ligne, puis on isole le dernier reste non nul et on remplace chaque reste par son expression tirée de la ligne précédente. Les erreurs de signe sont fréquentes. C'est pourquoi il faut toujours vérifier l'égalité finale par un calcul direct.

Quand peut-on simplifier une congruence ?

On peut diviser les deux membres de $ac \underset{[n]}{\equiv} bc$ par $c$ seulement si $c \wedge n = 1$, grâce au lemme de Gauss. Sinon la simplification est fausse : $2 \times 3 \underset{[10]}{\equiv} 2 \times 8$ alors que $3 \underset{[10]}{\not\equiv} 8$.

Le petit théorème de Fermat permet-il de prouver qu'un nombre est premier ?

Non. Il affirme que si $p$ est premier, alors $a^p \underset{[p]}{\equiv} a$, mais la réciproque est fausse. Par exemple, $2^{340} \underset{[341]}{\equiv} 1$ alors que $341 = 11 \times 31$. En revanche, il prouve qu'un nombre est composé dès qu'une puissance ne vérifie pas la congruence.

## Pour aller plus loin en L1

- Les énoncés : exercices de maths en L1 sur arithmétique dans Z
- Les solutions : corrigé des exercices sur arithmétique dans Z
- À maîtriser avant : Entiers naturels, récurrence et dénombrement
- Chapitre précédent : Fonctions usuelles et fonctions réciproques

- Chapitre suivant : Polynômes et fractions rationnelles
- Le sommaire : tous les chapitres de maths de L1 et la licence de maths de L1 à L3

Téléchargé depuis https://mathovore.fr - Mathovore site de maths.