

Arithmétique dans $\mathbb{Z}$

I. Arithmétique dans $\mathbb{Z}$: divisibilité et division euclidienne

Ce chapitre étudie les entiers relatifs sans aucun langage de structures. Tout repose sur deux outils : la division euclidienne et une propriété fondamentale de $\mathbb{N}$. En effet, toute partie non vide de $\mathbb{N}$ possède un plus petit élément. Cette propriété sert dans la plupart des démonstrations qui suivent.

Définition :

Soient $a, b \in \mathbb{Z}$. On dit que b **divise** a , et l'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 . L'ensemble des multiples de b se note $b\mathbb{Z}$.

Ainsi, tout entier divise 0 , alors que 0 ne divise que lui-même. De plus, b et $-b$ ont les mêmes diviseurs et les mêmes multiples. C'est pourquoi on se ramène souvent à des entiers positifs.

Propriété :

- La relation $\mid$ est réflexive et transitive sur $\mathbb{Z}$.
- Si $a \mid b$ et $b \mid a$, alors $|a| = |b|$.
- 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 :

Si $a = kd$ et $b = \ell d$, alors $au + bv = (ku + \ell v)d$. Ensuite, si $a = kb$ avec $a \neq 0$, alors $k \neq 0$, donc $|a| = |k||b| \geq |b|$. Enfin, si $a|b$ et $b|a$ avec $a \neq 0$, alors $b \neq 0$ et l'on obtient $|a| \leq |b| \leq |a|$. Le cas $a = 0$ impose $b = 0$.

Théorème :

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

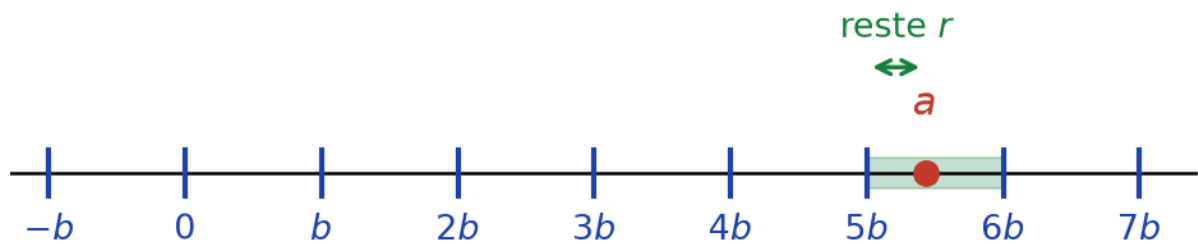
$$a = bq + r \text{ et } 0 \leq r < b.$$

L'entier q est le **quotient** et r le **reste**. De plus, $b|a$ si et seulement si $r = 0$.

Démonstration :

Existence : posons $q = \lfloor a/b \rfloor$. Alors $q \leq a/b < q + 1$, donc $bq \leq a < bq + b$. Par conséquent $r = a - bq$ vérifie $0 \leq r < b$. Unicité : si $bq + r = bq_1 + r_1$ avec les mêmes contraintes, alors $b|q - q_1| = |r_1 - r| < b$. Donc $|q - q_1| < 1$, d'où $q = q_1$ puis $r = r_1$.

Autrement dit, bq est le plus grand multiple de b inférieur ou égal à a , comme le montre la figure ci-dessous. Le reste mesure alors l'écart entre a et ce multiple.



ici $a = 38$, $b = 7$: $5b = 35 \leq a < 6b = 42$, donc $q = 5$ et $r = 3$

Exemple :

Divisons -58 par 9 . On a $-63 = 9 \times (-7)$ et $-63 \leq -58 < -54$. Donc $-58 = 9 \times (-7) + 5$: le quotient vaut -7 et le reste 5 . Attention, l'écriture $-58 = 9 \times (-6) - 4$ n'est pas la division euclidienne, car le reste doit être positif.

II. PGCD, algorithme d'Euclide et PPCM

1. Plus grand commun diviseur

Définition :

Soient $a, b \in \mathbb{Z}$ non tous deux nuls. L'ensemble de leurs diviseurs communs est fini et contient 1 . Son plus grand élément s'appelle le **PGCD** de a et b , noté $a \wedge b$. Par convention, $0 \wedge 0 = 0$.

Par exemple, les diviseurs positifs communs à 12 et 18 sont $1, 2, 3, 6$, donc $12 \wedge 18 = 6$. On a toujours $a \wedge b = |a| \wedge |b|$ et $a \wedge 0 = |a|$.

Lemme :

Si $a = bq + r$ avec $a, b, q, r \in \mathbb{Z}$, alors a et b ont les mêmes diviseurs communs que b et r . En particulier $a \wedge b = b \wedge r$.

Démonstration :

Un diviseur commun de a et b divise $r = a - bq$. Réciproquement, un diviseur commun de b et r divise $a = bq + r$. Les deux ensembles de diviseurs communs coïncident, donc leurs plus grands éléments aussi.

2. Algorithme d'Euclide

Le lemme conduit à un algorithme très efficace. On part de $r_0 = a$ et $r_1 = b$ avec $a \geq b > 0$. Ensuite, tant que $r_k \neq 0$, on note r_{k+1} le reste de la division de r_{k-1} par r_k . La suite des restes est strictement décroissante dans $\mathbb{N}$, donc elle atteint 0. Le dernier reste non nul est alors $a \wedge b$.

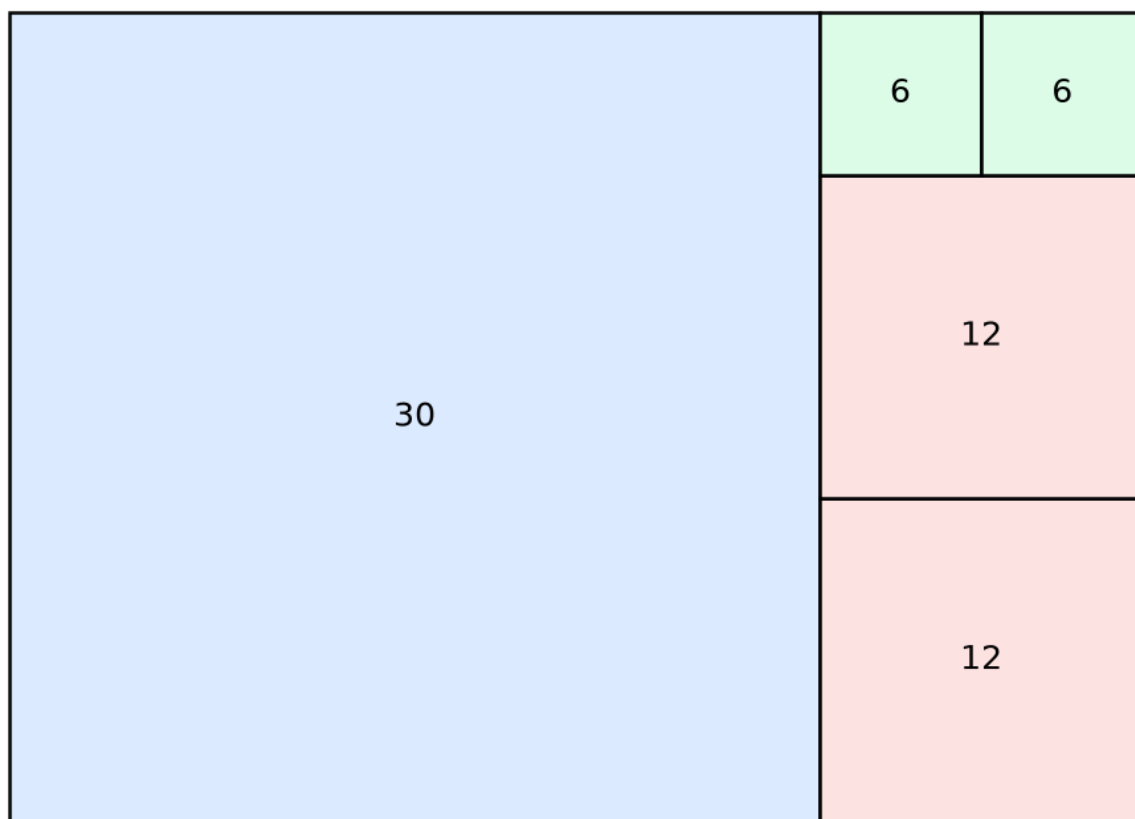
Méthode :

Pour calculer $a \wedge b$, enchaînez les divisions euclidiennes en remplaçant le couple (a, b) par (b, r) . Arrêtez-vous au premier reste nul : le PGCD est le reste précédent. Par exemple :

$$\begin{aligned} 42 &= 1 \times 30 + 12, \\ 30 &= 2 \times 12 + 6, \\ 12 &= 2 \times 6 + 0. \end{aligned}$$

Donc $42 \wedge 30 = 6$.

Cet algorithme possède une interprétation géométrique. On découpe un rectangle 42×30 en carrés les plus grands possibles, puis on recommence dans le rectangle restant. Ainsi, le côté du dernier carré est le PGCD, comme le montre la figure ci-dessous.



rectangle 42×30 : le dernier carré a pour côté $6 = 42 \wedge 30$

3. Plus petit commun multiple

Définition :

Soient $a, b \in \mathbb{Z}^*$. Le plus petit élément de $\mathbb{N}^*$ qui est multiple commun de a et b s'appelle le **PPCM** de a et b , noté $a \vee b$. Par convention, $a \vee 0 = 0$.

Propriété :

Pour tous $a, b \in \mathbb{Z}$, $d|a$ et $d|b$ équivaut à $d|a \wedge b$. De même, $a|m$ et $b|m$ équivaut à $a \vee b|m$. Enfin, pour $a, b \in \mathbb{N}$:

$$(a \wedge b)(a \vee b) = ab.$$

La première équivalence découle de la relation de Bézout, vue plus loin. La deuxième se prouve par division euclidienne de m par $a \vee b$: le reste est un multiple commun plus petit, donc il est nul. La formule du produit sera démontrée dans la partie V à l'aide des valuations.

III. Relation de Bézout et entiers premiers entre eux

1. Relation de Bézout

Théorème :

(Relation de Bézout) Soient $a, b \in \mathbb{Z}$. Il existe $u, v \in \mathbb{Z}$ tels que

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

Un tel couple (u, v) s'appelle un **couple de Bézout**. Il n'est pas unique.

Démonstration :

Suivons l'algorithme d'Euclide. Montrons par récurrence que chaque reste r_k s'écrit $au_k + bv_k$. C'est vrai pour $r_0 = a$ avec $(1, 0)$ et pour $r_1 = b$ avec $(0, 1)$. Ensuite, si $r_{k+1} = r_{k-1} - q_k r_k$, alors on pose $u_{k+1} = u_{k-1} - q_k u_k$ et $v_{k+1} = v_{k-1} - q_k v_k$. Le dernier reste non nul, égal à $a \wedge b$, est donc bien combinaison de a et b .

La démonstration fournit un calcul explicite. On l'appelle **algorithme d'Euclide étendu** et on le présente en tableau.

Méthode :

Pour trouver un couple de Bézout de a et b , écrivez trois colonnes r_k , u_k , v_k . Démarrez avec les lignes $(a, 1, 0)$ et $(b, 0, 1)$. Ensuite, chaque nouvelle ligne vaut « ligne d'avant-hier moins q_k fois ligne d'hier ». Par exemple, pour $a = 42$ et $b = 30$:

$$\begin{array}{c|ccc} q_k & r_k & u_k & v_k \\ \hline & 42 & 1 & 0 \\ & 30 & 0 & 1 \\ 1 & 12 & 1 & -1 \\ 2 & 6 & -2 & 3 \end{array}$$

On lit $42 \times (-2) + 30 \times 3 = 6$. Vérifiez toujours l'égalité finale.

2. Théorème de Bézout et lemme de Gauss

Définition :

Deux entiers a et b sont dits **premiers entre eux** si $a \wedge b = 1$, autrement dit si leurs seuls diviseurs communs sont 1 et -1 .

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 est la relation de Bézout. Réciproquement, si $au + bv = 1$, tout diviseur commun de a et b divise 1. Par conséquent $a \wedge b = 1$.

Théorème :

(Lemme de Gauss) Soient $a, b, c \in \mathbb{Z}$. Si $a \mid bc$ et $a \wedge b = 1$, alors $a \mid c$.

Démonstration :

Écrivons $au + bv = 1$. En multipliant par c , il vient $c = acu + bcv$. Or a divise acu et bcv , donc a divise c .

Corollaire :

- Si $a \mid n$, $b \mid n$ et $a \wedge b = 1$, alors $ab \mid n$.
- Si $a \wedge b = 1$ et $a \wedge c = 1$, alors $a \wedge bc = 1$.

- Si $d = a \wedge b \neq 0$, alors $a = da'$ et $b = db'$ avec $a' \wedge b' = 1$.

Attention :

L'hypothèse $a \wedge b = 1$ est indispensable. Par exemple, $6 \mid 4 \times 3$ mais 6 ne divise ni 4 ni 3. De même, $4 \mid 12$ et $6 \mid 12$ sans que 24 divise 12.

3. Équations diophantiennes linéaires

On cherche les couples d'entiers (x, y) tels que $ax + by = c$, avec a et b non nuls. Une telle équation est dite diophantienne.

Théorème :

L'équation $ax + by = c$ admet une solution entière si et seulement si $d = a \wedge b$ divise c . Dans ce cas, si (x_0, y_0) est une solution, et si $a = da'$, $b = db'$, l'ensemble des solutions est

$$\left\{ (x_0 + kb', y_0 - ka') \mid k \in \mathbb{Z} \right\}.$$

Démonstration :

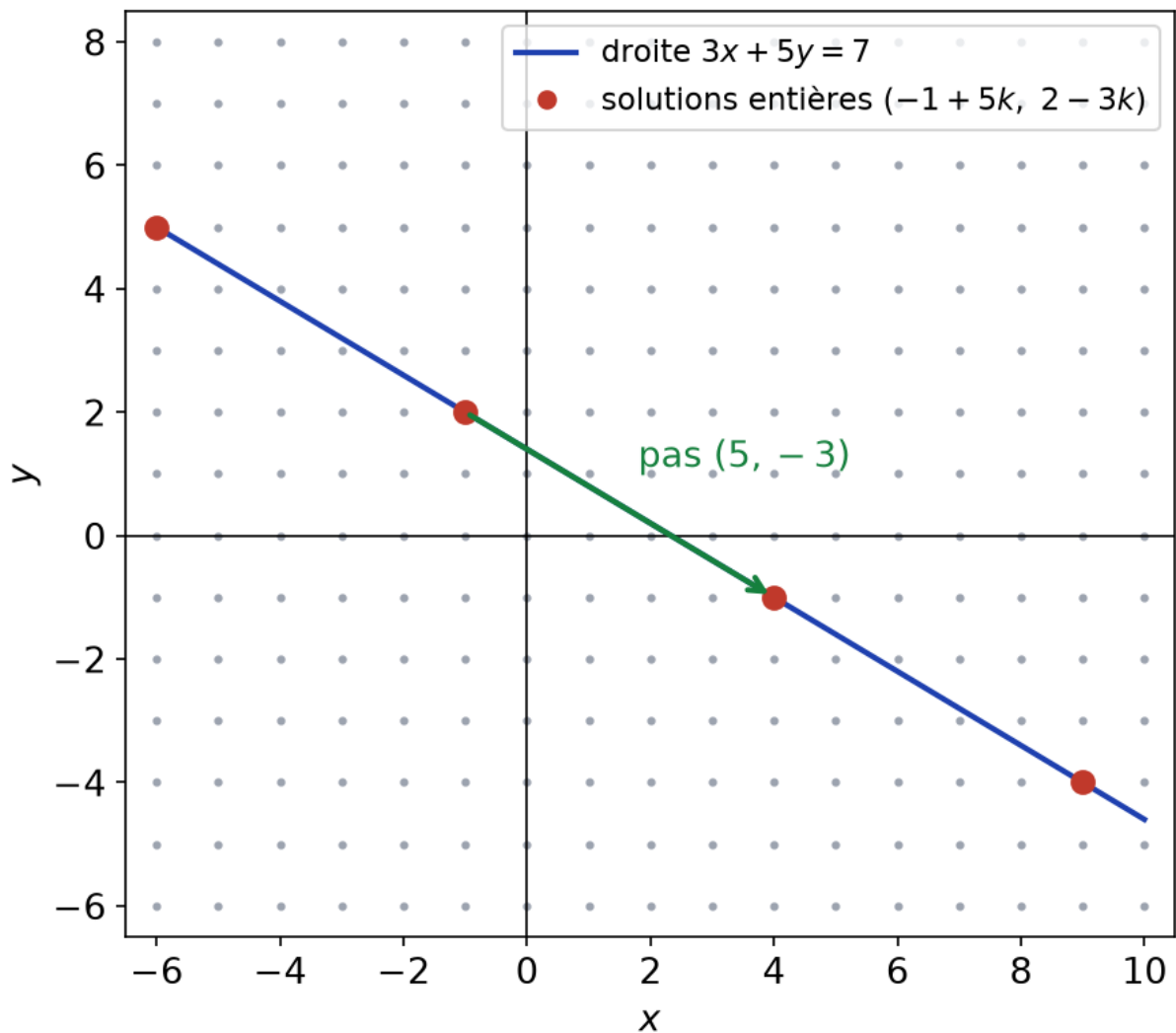
Si une solution existe, d divise $ax + by = c$. Réciproquement, si $c = dc'$, un couple de Bézout (u, v) donne la solution (uc', vc') . Ensuite, si (x, y) est solution, on soustrait :

$a(x - x_0) = -b(y - y_0)$. En divisant par d , on obtient $a'(x - x_0) = -b'(y - y_0)$. Or $a' \wedge b' = 1$, donc le lemme de Gauss donne $b' \mid x - x_0$. On écrit $x = x_0 + kb'$, puis on trouve $y = y_0 - ka'$. Enfin, ces couples sont bien solutions.

Exemple :

Réolvons $3x + 5y = 7$. D'abord, $3 \times 2 + 5 \times (-1) = 1$, donc $(14, -7)$ est solution. Une solution plus simple est $(-1, 2)$, car $-3 + 10 = 7$. Ainsi, les solutions sont les couples $(-1 + 5k, 2 - 3k)$ avec $k \in \mathbb{Z}$.

Géométriquement, les solutions sont les points à coordonnées entières de la droite d'équation $3x + 5y = 7$. Comme le montre la figure ci-dessous, elles sont régulièrement espacées, avec un pas $(5, -3)$.



4. PGCD d'un nombre fini d'entiers

Définition :

Le PGCD de $a_1, \dots, a_n$ est défini par récurrence :

$a_1 \wedge \dots \wedge a_n = (a_1 \wedge \dots \wedge a_{n-1}) \wedge a_n$. Les entiers sont **premiers entre eux dans leur ensemble** si ce PGCD vaut 1. Ils sont **premiers entre eux deux à deux** si $a_i \wedge a_j = 1$ pour tous $i \neq j$.

La relation de Bézout s'étend : il existe $u_1, \dots, u_n$ tels que

$a_1 u_1 + \dots + a_n u_n = a_1 \wedge \dots \wedge a_n$. En revanche, les deux notions de « premiers entre eux » diffèrent.

Exemple :

Les entiers $6, 10, 15$ sont premiers entre eux dans leur ensemble, car $6 + 10 - 15 = 1$. Cependant, ils ne sont pas premiers entre eux deux à deux, puisque $6 \wedge 10 = 2$. Enfin, si $a_1, \dots, a_n$ sont premiers entre eux deux à deux et divisent tous N , alors leur produit divise N .

IV. Nombres premiers

Définition :

Un entier $p \geq 2$ est **premier** si ses seuls diviseurs positifs sont 1 et p . On note $\mathcal{P}$ l'ensemble des nombres premiers.

Proposition :

- Tout entier $n \geq 2$ admet un diviseur premier.
- Si $n \geq 2$ n'est pas premier, il admet un diviseur premier p tel que $p^2 \leq n$.
- Si p est premier et $p \nmid a$, alors $p \wedge a = 1$.
- (Lemme d'Euclide) Si p est premier et $p \mid ab$, alors $p \mid a$ ou $p \mid b$.

Démonstration :

Le plus petit diviseur $d \geq 2$ de n existe et il est premier. En effet, un diviseur de d compris strictement entre 1 et d diviserait n . Si de plus $n = dm$ n'est pas premier, alors $m \geq d$, donc $d^2 \leq dm = n$. Ensuite, $p \wedge a$ divise p : il vaut 1 ou p , et il vaut 1 si

$p \nmid a$. Enfin, le lemme d'Euclide découle alors du lemme de Gauss.

Théorème :

(Euclide) L'ensemble des nombres premiers est infini.

Démonstration :

Supposons $\mathcal{P}$ fini, égal à $\{p_1, p_2, \dots, p_r\}$. Posons $N = p_1 p_2 \dots p_r + 1 \geq 2$.
D'après la proposition, N admet un diviseur premier p_i . Or p_i divise aussi le produit $p_1 \dots p_r$. Donc p_i divise 1, ce qui est absurde.

Pour lister les nombres premiers jusqu'à N , on utilise le **crible d'Ératosthène**. On écrit les entiers de 2 à N . Ensuite, on entoure 2 et on barre ses multiples. Puis on entoure le premier nombre non barré et on barre ses multiples, et ainsi de suite.

Méthode :

Dans le crible, il suffit de barrer les multiples des nombres premiers p tels que $p^2 \leq N$. En effet, un nombre composé $n \leq N$ possède un diviseur premier p avec $p^2 \leq n$. De plus, pour chaque p , on peut commencer à barrer à partir de p^2 . Pour $N = 100$, seuls 2, 3, 5, 7 servent.

La figure ci-dessous montre le crible pour $N = 100$. Chaque couleur indique le nombre premier qui a éliminé la case. On obtient ainsi les 25 nombres premiers inférieurs à 100.

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

nombre premier
 barré par 3
 barré par 7
 barré par 2
 barré par 5

V. Décomposition en facteurs premiers et valuations

Théorème :

(Théorème fondamental de l'arithmétique) Tout entier $n \geq 2$ s'écrit de façon unique, à l'ordre près des facteurs, comme produit de nombres premiers :

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

Démonstration :

Existence, par récurrence forte : si n est premier, c'est fini. Sinon $n = ab$ avec $2 \leq a, b < n$, et on concatène les décompositions de a et b . Unicité : supposons $p_1 \dots p_k = q_1 \dots q_\ell$ avec des facteurs premiers. Alors p_1 divise le produit des q_j . Par le lemme d'Euclide, il divise l'un d'eux, donc il lui est égal. On simplifie, puis on conclut par récurrence sur k .

Définition :

Soient p premier et $n \in \mathbb{Z}^*$. La **valuation p -adique** de n , notée $v_p(n)$, est le plus grand entier α tel que $p^\alpha \mid n$. Ainsi, $|n| = \prod_{p \in \mathcal{P}} p^{v_p(n)}$, produit dans lequel presque tous les exposants sont nuls.

Propriété :

Pour tous $a, b \in \mathbb{Z}^*$ et tout p premier :

- $v_p(ab) = v_p(a) + v_p(b)$;
- $a \mid b$ si et seulement si $v_p(a) \leq v_p(b)$ pour tout p premier ;
- $v_p(a \wedge b) = \min(v_p(a), v_p(b))$ et $v_p(a \vee b) = \max(v_p(a), v_p(b))$.

Démonstration :

La première égalité vient de l'unicité de la décomposition. Ensuite, si $b = ak$, alors $v_p(b) = v_p(a) + v_p(k) \geq v_p(a)$. Réciproquement, si les inégalités sont vraies, $k = \prod p^{v_p(b) - v_p(a)}$ convient. Enfin, un entier d divise a et b si et seulement si $v_p(d) \leq \min(v_p(a), v_p(b))$ pour tout p . Le plus grand est obtenu avec l'égalité. Le raisonnement est symétrique pour le PPCM.

Comme $\min(x, y) + \max(x, y) = x + y$, on retrouve $(a \wedge b)(a \vee b) = |ab|$. De même, deux entiers sont premiers entre eux si et seulement s'ils n'ont aucun facteur premier commun.

Exemple :

On a $360 = 2^3 \times 3^2 \times 5$ et $84 = 2^2 \times 3 \times 7$. Donc $360 \wedge 84 = 2^2 \times 3 = 12$ et $360 \vee 84 = 2^3 \times 3^2 \times 5 \times 7 = 2520$. On vérifie que $12 \times 2520 = 30240 = 360 \times 84$.

Remarque :

Pour les grands nombres, l'algorithme d'Euclide est bien plus rapide que la factorisation. En effet, on ne connaît pas d'algorithme efficace pour factoriser un entier de plusieurs centaines de chiffres. C'est d'ailleurs sur cette difficulté que repose le chiffrement RSA.

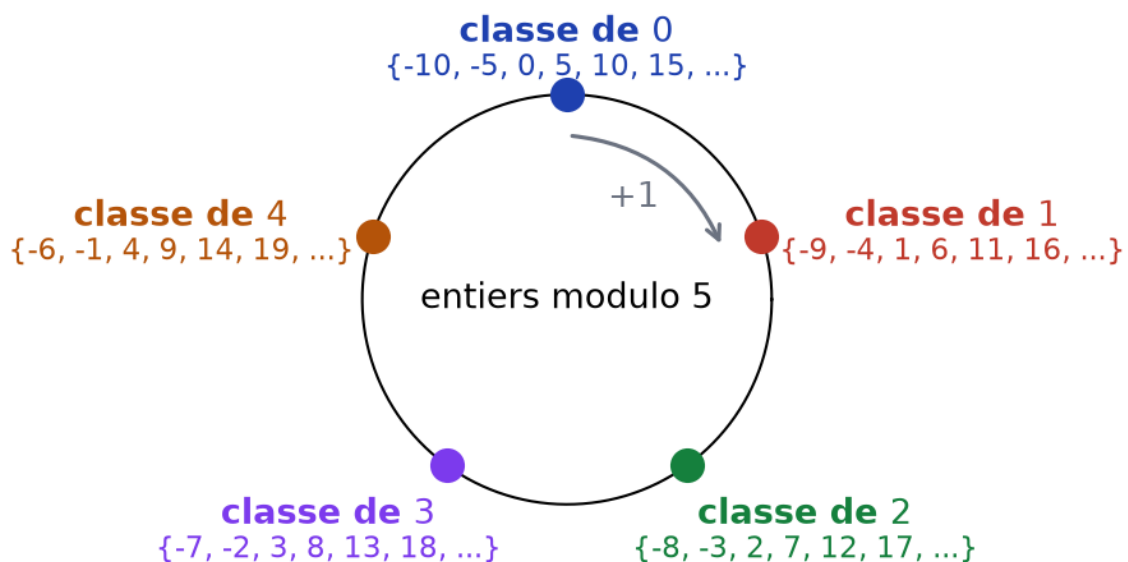
VI. Congruences modulo n et petit théorème de Fermat

1. Congruences

Définition :

Soit $n \in \mathbb{N}^*$. On dit que a est **congru** à b modulo n , et l'on note $a \equiv b \pmod{n}$, si $n \mid a - b$.
De façon équivalente, a et b ont le même reste dans la division euclidienne par n .

La congruence modulo n est une relation d'équivalence. Tout entier est congru à exactement un entier de $\{0, 1, \dots, n-1\}$, son reste. Ainsi, on peut « enrouler » les entiers sur un cercle à n positions, comme le montre la figure ci-dessous pour $n = 5$.



Propriété :

Si $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n}$, alors $a + c \equiv b + d \pmod{n}$ et $ac \equiv bd \pmod{n}$. Par conséquent, $a^k \equiv b^k \pmod{n}$ pour tout $k \in \mathbb{N}$.

Démonstration :

On a $(a + c) - (b + d) = (a - b) + (c - d)$, qui est multiple de n . Ensuite, $ac - bd = a(c - d) + d(a - b)$, qui est aussi multiple de n . La propriété sur les puissances s'obtient par récurrence sur k .

Attention :

On ne simplifie pas une congruence comme une égalité. Par exemple, $\frac{2 \times 3}{10} \equiv \frac{2 \times 8}{10}$, mais $\frac{3}{10} \not\equiv \frac{8}{10}$. La simplification par a n'est permise que si $a \wedge n = 1$.

2. Inverse modulo n

Définition :

Un entier a est **inversible modulo n** s'il existe $u \in \mathbb{Z}$ tel que $\frac{au}{n} \equiv 1$. Un tel u s'appelle un inverse de a modulo n .

Théorème :

L'entier a est inversible modulo n si et seulement si $a \wedge n = 1$. Dans ce cas, pour tout b , la congruence $\frac{ax}{n} \equiv b$ équivaut à $\frac{x}{n} \equiv ub$, où u est un inverse de a .

Démonstration :

Dire que $au \equiv 1 \pmod{n}$, c'est dire qu'il existe v tel que $au + nv = 1$. D'après le théorème de Bézout, cela équivaut à $a \wedge n = 1$. Ensuite, si $ax \equiv b$, on multiplie par u et l'on obtient $x \equiv ub$. Réciproquement, si $x \equiv ub$, alors $ax \equiv aub \equiv b$.

Exemple :

Réolvons $7x \equiv 3 \pmod{12}$. D'abord, $7 \times 7 = 49 = 4 \times 12 + 1$, donc 7 est son propre inverse modulo 12 . Par conséquent $x \equiv 21 \equiv 9 \pmod{12}$. On vérifie : $7 \times 9 = 63 = 5 \times 12 + 3$.

3. Petit théorème de Fermat

Lemme :

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

Démonstration :

On a $k \binom{p}{k} = p \binom{p-1}{k-1}$. Ainsi, p divise $k \binom{p}{k}$. Or $p \wedge k = 1$ puisque $1 \leq k < p$. Le lemme de Gauss donne donc $p \mid \binom{p}{k}$.

Théorème :

(Petit théorème de Fermat) Soit p un nombre premier. Pour tout $a \in \mathbb{Z}$, on a $a^p \equiv a \pmod{p}$. Si de plus $p \nmid a$, alors

$$a^{p-1} \equiv 1 \pmod{p}.$$

Démonstration :

Montrons $a^p \equiv a$ par récurrence pour $a \in \mathbb{N}$. C'est clair pour $a = 0$. Ensuite, la formule du binôme et le lemme donnent $(a+1)^p \equiv a^p + 1 \pmod{p}$. Donc $(a+1)^p \equiv a+1$ si $a^p \equiv a$. Pour $a < 0$, on remplace a par un entier positif qui lui est congru. Enfin, si $p \nmid a$, alors $p \wedge a = 1$, et l'on simplifie $a \cdot a^{p-1} \equiv a \cdot 1 \pmod{p}$ par a .

La table ci-dessous donne les restes de a^k modulo 7. La colonne $k = 6$ ne contient que des 1, conformément au théorème. De plus, les restes se répètent avec une période qui divise 6.

$k = 6 = p - 1$

$a = 1$	1	1	1	1	1	1	1	1	1	1	1	1
$a = 2$	2	4	1	2	4	1	2	4	1	2	4	1
$a = 3$	3	2	6	4	5	1	3	2	6	4	5	1
$a = 4$	4	2	1	4	2	1	4	2	1	4	2	1
$a = 5$	5	4	6	2	3	1	5	4	6	2	3	1
$a = 6$	6	1	6	1	6	1	6	1	6	1	6	1
	1	2	3	4	5	6	7	8	9	10	11	12

exposant k : case = reste de a^k modulo 7

Méthode :

Pour réduire a^N modulo un premier p ne divisant pas a , faites la division euclidienne

$N = (p-1)q + r$. Alors $a^N = (a^{p-1})^q a^r \equiv a^r \pmod{p}$. Par exemple,
 $3^{100} \equiv 3^4 = 81 \equiv 4 \pmod{7}$, car $100 = 6 \times 16 + 4$.

Remarque :

Le théorème fournit aussi un inverse : si $p \nmid a$, alors a^{p-2} est un inverse de a modulo p . Cependant, l'algorithme d'Euclide étendu reste en général plus rapide. Hors programme, le théorème se généralise en $a^{\varphi(n)} \equiv 1 \pmod{n}$ lorsque $a \wedge n = 1$, résultat étudié en spé.

Ce qu'il faut retenir

- La division euclidienne $a = bq + r$, $0 \leq r < b$, existe et est unique : c'est l'outil de base du chapitre.
- L'algorithme d'Euclide repose sur $a \wedge b = b \wedge r$; le dernier reste non nul est le PGCD.
- La relation de Bézout $au + bv = a \wedge b$ se calcule par l'algorithme d'Euclide étendu.
- Théorème de Bézout : $a \wedge b = 1$ si et seulement si $au + bv = 1$ pour certains entiers u, v .
- Lemme de Gauss : si $a \mid bc$ et $a \wedge b = 1$, alors $a \mid c$. Il sert à résoudre $ax + by = c$.
- L'ensemble des nombres premiers est infini ; le crible d'Ératosthène les liste jusqu'à N en barrant les multiples des $p \leq \sqrt{N}$.
- La décomposition en facteurs premiers est unique ; PGCD et PPCM s'obtiennent par $\min$ et $\max$ des valuations.

- Les congruences sont compatibles avec la somme et le produit, mais on ne simplifie que par un entier premier avec n .
- L'entier a est inversible modulo n si et seulement si $a \wedge n = 1$.
- Petit théorème de Fermat : $a^p \equiv a \pmod{p}$, et $a^{p-1} \equiv 1 \pmod{p}$ si $p \nmid a$.

Questions fréquentes sur arithmétique dans $\mathbb{Z}$

Comment trouver un couple de Bézout rapidement ?

Utilisez l'algorithme d'Euclide étendu présenté en tableau, avec les colonnes r_k , u_k et v_k . Chaque ligne vaut la ligne d'avant-hier moins le quotient fois la ligne d'hier. Vérifiez toujours l'égalité $au + bv = a \wedge b$ à la fin, car une erreur de signe est vite arrivée.

Quelle différence entre premiers entre eux dans leur ensemble et deux à deux ?

Des entiers sont premiers entre eux dans leur ensemble si leur PGCD global vaut 1. Ils le sont deux à deux si chaque paire a un PGCD égal à 1, ce qui est plus fort. Par exemple, 6, 10 et 15 sont premiers entre eux dans leur ensemble, mais pas deux à deux.

Quand peut-on simplifier une congruence ?

On peut simplifier $ax \equiv ay \pmod{n}$ par a seulement si $a \wedge n = 1$, car a est alors inversible modulo n . Sinon, la simplification est fautive : $2 \times 3 \equiv 2 \times 8 \pmod{10}$ alors que 3 et 8 ne sont pas congrus modulo 10.

À quoi sert le petit théorème de Fermat en pratique ?

Il permet de réduire les exposants : si p est premier et ne divise pas a , alors $a^{p-1} \equiv 1 \pmod{p}$. On divise donc l'exposant par $p - 1$ et on ne garde que le reste. Il fournit aussi un inverse modulo p et fonde le chiffrement RSA.

Pour aller plus loin en maths sup

- Les énoncés : [exercices de maths sup sur arithmétique dans \$\mathbb{Z}\$](#)
- À maîtriser avant : [Logique, ensembles, applications et relations](#)
- Chapitre précédent : [Dérivabilité et convexité](#)
- Chapitre suivant : [Structures algébriques usuelles : groupes, anneaux, corps](#)
- Le même thème en L1 : [arithmétique dans \$\mathbb{Z}\$, cours de maths en L1](#)
- Tester vos connaissances : [QCM de maths sup par chapitre](#)
- Le sommaire : [tous les chapitres de maths sup](#) et les [chapitres de maths spé](#)