Lycée Henri IV
MPSI

Cours
Durée : 8 h

ARITHMÉTIQUE

Les énoncés et parties suivis du symbole [✠] ne seront pas traités en cours.

Prérequis

Revoir les chapitres sur :

- les nombres ;
- les relations ;
- les structures algébriques.

Les trois lettres AQT signifient « Âne Qui Trotte » et sont utilisées pour désigner une démonstration facile laissée au lecteur.

A. Divisibilité

A.1. Multiples et diviseurs d'un entier

Définition 1

Soient $a, b \in \mathbb{Z}$. On dit que b divise a et l'on note $b \mid a$ s'il existe $q \in \mathbb{Z}$ tel que $a = bq$.
On dit alors que b est un diviseur de a et que a est un multiple de b.
L'ensemble des diviseurs de a est noté $\mathscr{D}(a)$ et celui des multiples de b est noté $b\mathbb{Z}$ ou $\mathscr{M}(b)$.

Exemples :

- Tout entier divise 0 ou, ce qui revient au même, 0 est un multiple de tout entier. En effet, $\forall b \in \mathbb{Z},\ 0 = b \times 0$.
- Les entiers 1 et -1 divisent tout autre entier puisque $\forall a \in \mathbb{Z},\ a = \pm 1 \times (\mp a)$.
- Il existe un critère très simple pour savoir si un nombre entier a est divisible par 2 : il suffit de regarder si le chiffre des unités de a appartient à $\{0; 2; 4; 6; 8\}$. Pour 4, le critère n'est guère plus compliqué : a est divisible par 4 si le nombre formé des deux derniers chiffres de a est divisible par 4. Plus généralement, a est divisible par 2^ℓ si le nombre formé des ℓ derniers chiffres de a est divisible par 2^ℓ.

  Le critère de divisibilité de 5 est de même nature : a est divisible par 5^ℓ si le nombre formé des ℓ derniers chiffres de a est divisible par 5^ℓ.

  Pour 3, il suffit de regarder si la somme des chiffres de a est divisible par 3 pour conclure la même chose à propos de a (quitte, si le résultat est trop grand, à réappliquer le critère...).

  Pour savoir si un entier a est divisible par 11, on fait la différence entre la somme des chiffres de positions paires et la somme des chiffres de positions impaires et l'on regarde si le résultat est divisible par 11. La réponse est la même pour a.

  On peut se demander s'il existe un critère de divisibilité pour tous les nombres premiers. La réponse est positive ! Nous verrons en exercice que cela découle du principe des tiroirs.

La divisibilité établit une relation d'ordre sur $\mathbb{N}$ et de préordre sur $\mathbb{Z}$.

Proposition 1

Restreintes à $\mathbb{N}$, les relations « divise » et « est multiple de » sont des relations d'ordre partiel, c'est-à-dire

$$\begin{aligned}
&\text{(i)} && \forall a \in \mathbb{N},\quad a \mid a && \text{(réflexivité)};\\
&\text{(ii)} && \forall a, b \in \mathbb{N},\quad (a \mid b \text{ et } b \mid a) \Longrightarrow (a = b) && \text{(antisymétrie)};\\
&\text{(iii)} && \forall a, b, c \in \mathbb{N},\quad (a \mid b \text{ et } b \mid c) \Longrightarrow (a \mid c) && \text{(transitivité)}.
\end{aligned}$$

Sur $\mathbb{Z}$, ces relations ne sont pas des relations d'ordre car, si les propriétés (i) et (iii) restent vraies, la propriété d'antisymétrie tombe en défaut. On a seulement :

$$\text{(ii)'}\quad \forall a, b \in \mathbb{Z},\quad (a \mid b \text{ et } b \mid a) \Longleftrightarrow (a = \pm b) \quad (a \text{ et } b \text{ sont dits associés}).$$

■ AQT ■

Cette proposition implique que $\big(\mathscr{D}(b) \subset \mathscr{D}(a)\big) \iff (b \mid a) \iff (a\mathbb{Z} \subset b\mathbb{Z})$.

Deux entiers associés ont souvent les mêmes propriétés de divisibilité. Par conséquent, en pratique, on préfère souvent utiliser celui des deux qui est positif.

Sur $\mathbb{N}$, la divisibilité est une relation d'ordre « plus forte » que $\leqslant$ au sens où, pour tout $a \in \mathbb{N}$ et tout $b \in \mathbb{N}^*$, on a $(a \mid b) \Longrightarrow (a \leqslant b)$. Cette remarque évidente a le mérite de faire le lien entre la relation d'ordre naturelle et la divisibilité, qui est la relation d'ordre (ou de préordre) privilégiée lorsqu'on fait de l'arithmétique sur $\mathbb{N}$ (ou sur $\mathbb{Z}$).

L'énoncé suivant complète les propriétés élémentaires de la relation de divisibilité dans $\mathbb{Z}$.

Proposition 2

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

(i) si $b \mid a$ et $b \mid c$ alors $b \mid a + c$;

(ii) si $b \mid a$ et $d \mid c$ alors $bd \mid ac$.

En particulier, la propriété (ii) nous dit que

(ii)' pour tout $p \in \mathbb{N}$, si $b \mid a$ alors $b^p \mid a^p$.

■ AQT ■

La propriété (i) énonce la stabilité de la divisibilité par addition. Si l'on combine cette propriété avec la transitivité de la divisibilité et une simple récurrence, on obtient que si l'entier b divise les entiers $a_1, \ldots, a_n$ alors pour tous entiers $m_1, \ldots, m_n$, l'entier b divise $m_1 a_1 + \cdots + m_n a_n$. On dit alors que la divisibilité est stable par combinaison linéaire à coefficients dans $\mathbb{Z}$.

Attention, la stabilité de la divisibilité par addition vaut pour l'addition des multiples, pas des diviseurs ! Ainsi, 2 et 3 divisent 6 mais $2 + 3 = 5$ ne divise pas 6.

A.2. Division euclidienne

Le résultat suivant généralise celui que l'on avait énoncé pour les entiers naturels.

Théorème 1

Soient $a, b \in \mathbb{Z}$ avec $b \neq 0$. Il existe un unique couple $(q, r) \in \mathbb{Z}^2$ tel que

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

Les nombres entiers q et r s'appellent respectivement le quotient et le reste de la division euclidienne du dividende a par le diviseur b.

■ ▷ Existence : L'ensemble $E = \{m \in b\mathbb{Z} : m \leqslant a\}$ des multiples de b inférieurs ou égaux à a est une partie non vide (y réfléchir) de $\mathbb{Z}$ majorée par a. Il possède donc un plus grand élément, que nous noterons bq. Posons $r = a - bq$. Comme $bq \leqslant a$, on a $r \geqslant 0$. De plus, $bq + |b|$ est un multiple de b supérieur à bq, donc $bq + |b| > a$, d'où $r < |b|$.

▷ Unicité : Supposons que $a = bq + r = bq' + r'$ avec $0 \leqslant r < |b|$ et $0 \leqslant r' < |b|$. On a $b(q - q') = r' - r$ donc $r' - r$ est un multiple de b. Comme $r - r'$ est compris entre $-|b|$ et $|b|$, il ne peut être que nul. Donc $r = r'$ et par conséquent $q = q'$. ■

En pratique (en particulier quand on calcule avec des congruences), le diviseur est presque toujours positif, c'est-à-dire $b \in \mathbb{N}^*$. Par contre, le dividende a est parfois positif, parfois négatif.

Lorsque $|b| > |a|$, on a $a = b.0 + a$.

Lorsque $b \in \mathbb{N}^*$, le quotient q de la division euclidienne de a par b est donné par

$$q = \left\lfloor \frac{a}{b} \right\rfloor.$$

En effet, comme $0 \leqslant r < b$, on a $0 \leqslant a - bq < b$, c'est-à-dire $a/b - 1 < q \leqslant a/b$, d'où $q = \lfloor a/b \rfloor$.

Pour trouver q, il suffit donc de demander à sa boutonneuse la valeur du quotient a/b et de retenir la partie entière d'icelui.

Exemples :

- La division euclidienne de 1975 par 17 donne $1975 = 116 \times 17 + 3$.
- La division euclidienne de -1975 par 17 n'est pas $-1975 = -116 \times 17 - 3$ puisque le reste doit être positif. On rajoute 17 au reste et on compense en retirant 1 au quotient (ce qui revient à oter 1 fois 17). On obtient $-1975 = -117 \times 17 + 14$.

  D'ailleurs, la calculatrice donne $-1975/17 \approx -116,2$ dont la partie entière est bien -117.

Nous pouvons faire un lien immédiat entre la divisibilité d'un entier par un autre et le reste obtenu dans la division euclidienne.

Corollaire 1

Soient $a, b \in \mathbb{Z}$ avec $b \neq 0$. Le nombre b divise le nombre a si, et seulement si, le reste de la division euclidienne de a par b est nul.

■ AQT ■

L'existence de la division euclidienne entre entiers confère à $\mathbb{Z}$ une structure d'anneau dit euclidien. C'est cette caractéristique qui est à la base de la plupart des propriétés arithmétiques de $\mathbb{Z}$.

Nous rencontrerons en cours d'année un autre anneau euclidien : celui des polynômes. On pourra donc, là aussi, faire de l'arithmétique !

B. Diviseurs et multiples communs

B.1. Plus grand diviseur commun

a) Plus grand diviseur commun de deux entiers

Définition 2

Soient a et b deux nombres entiers relatifs. Le pgcd de a et b, noté $a \wedge b$ ou $\text{pgcd}(a,b)$, est

(i) le plus grand des diviseurs communs à a et b lorsque $(a,b) \neq (0,0)$;

(ii) égal à 0 lorsque a et b sont nuls.

■ Si $(a,b) \neq (0,0)$, l'ensemble des diviseurs communs à a et b est une partie de $\mathbb{Z}$, non vide (puisqu'elle contient 1) et majorée par $\max\{|a|,|b|\}$. Elle possède donc bien un plus grand élément. ■

Notons que le pgcd est insensible aux signes de a et b puisque $a \wedge b = |a| \wedge |b|$ ainsi qu'à l'ordre de a et b puisque $a \wedge b = b \wedge a$. Par conséquent, on peut toujours supposer que $0 \leqslant b \leqslant a$.

Le pgcd est par exemple utile pour la simplification de l'écriture fractionnaire d'un nombre rationnel : pour simplifier une fraction, on divise numérateur et dénominateur par leur pgcd.

Exemples :

- Pour tout $a \in \mathbb{Z}$, on a $a \wedge 0 = |a|$. Sur $\mathbb{N}$, 0 est un élément neutre pour la loi $\wedge$.
- Pour tout $a \in \mathbb{Z}$, on a $a \wedge 1 = 1$. Sur $\mathbb{Z}$, 1 est un élément absorbant pour la loi $\wedge$.

À ce stade, le pgcd est un outil arithmétique peu commode. En effet, par définition, le pgcd de deux entiers est le diviseur commun le plus grand au sens de la relation d'ordre usuelle $\leqslant$. Ainsi, si d désigne un diviseur commun quelconque de a et b, on peut seulement affirmer, pour l'instant, que $d \leqslant a \wedge b$. Les résultats qui suivent vont nous permettre d'établir que le pgcd est aussi le diviseur commun le plus grand au sens de la relation d'ordre de divisibilité sur $\mathbb{N}$. Ainsi, lorsque d désignera un diviseur commun quelconque de a et b, on pourra affirmer que $d \mid a \wedge b$.

Commençons par établir un lemme qui généralise l'équivalence $\big(\mathscr{D}(b) \subset \mathscr{D}(a)\big) \iff (b \mid a)$.

Lemme 1

Soient $a, b \in \mathbb{Z}$ tels que $b \neq 0$. Si l'on a $a = bq + r$ (en particulier, lorsqu'on fait une division euclidienne), alors l'ensemble des diviseurs communs de a et b est aussi l'ensemble des diviseurs communs de b et r, c'est-à-dire

$$\mathscr{D}(a) \cap \mathscr{D}(b) = \mathscr{D}(b) \cap \mathscr{D}(r).$$

En particulier,

$$a \wedge b = b \wedge r.$$

■ Si $d \in \mathscr{D}(a) \cap \mathscr{D}(b)$, alors $d \mid bq$ et $d \mid a$, donc $d \mid (a - bq) = r$. Par conséquent, $d \in \mathscr{D}(b) \cap \mathscr{D}(r)$.
Si $d \in \mathscr{D}(b) \cap \mathscr{D}(r)$, alors $d \mid bq$ et $d \mid r$, donc $d \mid bq + r = a$. Par conséquent, $d \in \mathscr{D}(a) \cap \mathscr{D}(b)$.
Les plus grands éléments de $\mathscr{D}(a) \cap \mathscr{D}(b)$ et $\mathscr{D}(b) \cap \mathscr{D}(r)$ sont donc égaux, d'où $a \wedge b = b \wedge r$. ■

On voit bien tout l'intérêt de cet énoncé : il ramène le calcul du pgcd d'un couple de nombres à celui d'un autre couple dont l'un des deux nombres est plus petit. C'est cette remarque que l'algorithme d'Euclide (que nous verrons plus loin) exploite pour le calcul du pgcd.

Le lemme précédent permet de déterminer l'intersection de deux ensembles de diviseurs, c'est-à-dire un ensemble de diviseurs communs.

Proposition 3

Soient $a, b \in \mathbb{Z}$. L'ensemble des diviseurs communs de a et b est aussi l'ensemble des diviseurs du pgcd de a et b, c'est-à-dire

$$\mathscr{D}(a) \cap \mathscr{D}(b) = \mathscr{D}(a \wedge b).$$

■ Les cas où $a = 0$ ou $b = 0$ sont triviaux.

On pose $r_0 = a$ et $r_1 = b$. Pour tout $n \in \mathbb{N}^*$ tel que $r_{n-1} \neq 0$, on note r_{n+1} le reste de la division euclidienne de r_{n-1} par r_n. D'après le lemme 1, on a

$$\mathscr{D}(a) \cap \mathscr{D}(b) = \mathscr{D}(b) \cap \mathscr{D}(r_2) = \mathscr{D}(r_2) \cap \mathscr{D}(r_3) = \cdots = \mathscr{D}(r_N) \cap \mathscr{D}(0) = \mathscr{D}(r_N)$$

où la présence d'un reste nul est assurée par le fait la suite des r_k est une suite strictement décroissante d'entiers naturels, qui finit donc nécessairement par s'arréter à la valeur 0.

Les plus grands éléments de $\mathscr{D}(a) \cap \mathscr{D}(b)$ et $\mathscr{D}(r_N)$ sont donc égaux, d'où $a \wedge b = r_N$, ce qui donne le résultat attendu. ■

Ce résultat signifie que $a \wedge b$ est le plus grand, au sens de la divisibilité, des diviseurs positifs communs à a et b.(†)

C'est même valable lorsque $a = b = 0$ car dans ce cas, l'ensemble des diviseurs positifs communs est égal à $\mathbb{N}$ et 0 est bien le plus grand élément de $\mathbb{N}$ pour la divisibilité.

On retiendra donc que

un entier d divise a et b si, et seulement si, d divise $a \wedge b$.

On utilise quelquefois ce résultat pour déterminer le pgcd de deux entiers a et b lorsque l'on connait un candidat potentiel pour le rôle. Pour cela, on montre que ce candidat δ divise a et b puis que tout diviseur d de a et b est un diviseur de δ.

(†) Pour la relation de divisibilité, un minorant est un diviseur. Par conséquent, $a \wedge b$ est le plus grand des minorants de $\{a; b\}$, c'est-à-dire que $a \wedge b$ est la borne inférieure de $\{a; b\}$.

b) Coefficients de Bézout

Proposition 4

Soient $a, b \in \mathbb{Z}$. Il existe des couples $(u, v) \in \mathbb{Z}^2$, appelés couples de coefficients de Bézout de a et b, tels que

$$ua + vb = a \wedge b.$$

Autrement dit,

$$a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\mathbb{Z}.$$

■ Deux démonstrations pour le prix d'une !

▷ Première démonstration : Avec des idéaux

Les ensembles $a\mathbb{Z}$ et $b\mathbb{Z}$ sont des idéaux de $\mathbb{Z}$, donc $a\mathbb{Z} + b\mathbb{Z}$ est aussi un idéal de $\mathbb{Z}$ (c'est l'idéal engendré par $a\mathbb{Z}$ et $b\mathbb{Z}$). Comme les idéaux de $\mathbb{Z}$ sont tous de la forme $n\mathbb{Z}$ avec $n \in \mathbb{N}^*$, on en déduit l'existence de $\delta \in \mathbb{N}^*$ tel que $a\mathbb{Z} + b\mathbb{Z} = \delta\mathbb{Z}$.

Comme $a\mathbb{Z}$ et $b\mathbb{Z}$ sont inclus dans $a\mathbb{Z} + b\mathbb{Z}$, on a $a\mathbb{Z} \subset \delta\mathbb{Z}$ et $b\mathbb{Z} \subset \delta\mathbb{Z}$, ce qui signifie que $\delta \mid a$ et $\delta \mid b$. Il s'ensuit que $\delta \mid a \wedge b$.

Par ailleurs, comme $(a \wedge b) \mid a$ et $(a \wedge b) \mid b$, on a $a\mathbb{Z} \subset (a \wedge b)\mathbb{Z}$ et $b\mathbb{Z} \subset (a \wedge b)\mathbb{Z}$ et donc $a\mathbb{Z} + b\mathbb{Z} \subset (a \wedge b)\mathbb{Z}$ ou encore $\delta\mathbb{Z} \subset (a \wedge b)\mathbb{Z}$. Donc $a \wedge b \mid \delta$.

Donc $\delta = a \wedge b$, ce qui donne $a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\mathbb{Z}$.

▷ Seconde démonstration : avec une récurrence forte

Quitte à remplacer a par $|a|$, b par $|b|$ et à changer les signes des coefficients u et v, il suffit de traiter le cas où a et b sont des nombres entiers naturels. Pour tout $b \in \mathbb{N}$, on pose

$$\mathscr{P}_b : \quad \forall a \in \mathbb{N}, \quad \exists (u, v) \in \mathbb{Z}^2, \qquad ua + vb = a \wedge b.$$

Initialisation : La propriété $\mathscr{P}_0$ est vraie car, pour tout $a \in \mathbb{N}$, on a $a \wedge 0 = a = 1 \times a + 0 \times 0$.

Hérédité : Fixons $b \geqslant 1$ tel que $\mathscr{P}_0, \ldots, \mathscr{P}_{b-1}$ sont vraies et démontrons $\mathscr{P}_b$. Soit $a \in \mathbb{N}$. Notons d le pgcd de a et b. On effectue la division euclidienne de a par b, ce qui donne $a = bq + r$ avec $0 \leqslant r < b$. D'après le lemme 1, on a donc $d = b \wedge r$ et la propriété $\mathscr{P}_r$ justifie l'existence de $(\alpha, \beta) \in \mathbb{Z}^2$ tels que $\alpha b + \beta r = d$. Mézalors $b\alpha + (a - bq)\beta = d$, ce qui donne $b(\alpha - q\beta) + a\beta = d$. On pose $u = \beta$ et $v = \alpha - q\beta$, ce qui prouve $\mathscr{P}_b$.

Conclusion : Le principe de récurrence permet de conclure. ■

Il n'y a pas du tout unicité des coefficients de Bézout. En fait, si (u, v) est un couple de Bézout, alors les couples $(u - kb, v + ka)$ où $k \in \mathbb{Z}$ sont d'autres couples de Bézout (d'après Binet !).

Cette proposition permet aussi d'établir la distributivité, dans $\mathbb{N}$, du produit sur le pgcd.

Proposition 5

Soient $k \in \mathbb{N}$ et $a, b \in \mathbb{Z}$. On a

$$k(a \wedge b) = ka \wedge kb.$$

En particulier, si d est un diviseur strictement positif de a et b, on a

$$\frac{a}{d} \wedge \frac{b}{d} = \frac{a \wedge b}{d}.$$

■ On a $k(a \wedge b)\mathbb{Z} = k(a\mathbb{Z} + b\mathbb{Z}) = ka\mathbb{Z} + kb\mathbb{Z} = (ka \wedge kb)\mathbb{Z}$, d'où $k(a \wedge b) = ka \wedge kb$. ■

En particulier, si l'on choisit $d = a \wedge b$ (avec $ab \neq 0$) dans la seconde formule de cette proposition, on constate qu'en divisant a et b par leur pgcd, on obtient deux nombres dont le pgcd est 1 (c'est-à-dire des nombres premiers entre eux). Nous utiliserons cette remarque pour caractériser le pgcd dans la proposition 6.

C'est aussi cette remarque qui permet de simplifier une fraction pour obtenir le représentant irréductible d'un rationnel. Nous y reviendrons dans le corollaire 2.

c) *Algorithme d'Euclide*

Nous décrivons dans ce paragraphe l'algorithme d'Euclide pour le calcul du pgcd et des coefficients de Bézout. Cette méthode repose sur la démonstration de la proposition 3.

Algorithme d'Euclide

Disons que l'on veuille déterminer le pgcd de deux nombres entiers a et b avec $b \neq 0$. Par exemple $a = 70$ et $b = 6$

On pose $r_0 = a$ et $r_1 = b$ et l'on dispose les calculs sous forme d'un tableau

i	q_i	r_i	u_i	v_i
0		a	1	0
1		b	0	1

q_i	r_i	u_i	v_i
	70	1	0
	6	0	1

dont la première colonne (facultative) indique le numéro i de l'étape de l'algorithme, la deuxième colonne est celle des quotients q_i successifs que l'on va déterminer (pour l'instant cette colonne est vide), la troisième colonne est celle des restes r_i (elle contient pour l'instant a et b) et les deux dernières colonnes contiennent les coefficients de Bézout u_i et v_i, c'est-à-dire les nombres entiers tels que $r_i = u_i a + v_i b$.

On effectue ensuite la division euclidienne de a par b, de sorte que $a = bq + r$. On pose alors $q_1 = q$, $r_2 = r$ et l'on calcule $u_2 = u_0 - q_1 u_1$ et $v_2 = v_0 - q_1 v_1$.

i	q_i	r_i	u_i	v_i
0		a	1	0
1	q_1	b	0	1
2		r_2	1	$-q_1$

q_i	r_i	u_i	v_i
	70	1	0
11	6	0	1
	4	1	−11

On poursuit ensuite le processus tant que l'on voit apparaître des restes non nuls : pour $n \geqslant 1$, si $r_n \neq 0$, r_{n+1} est le reste de la division euclidienne de r_{n-1} par r_n, q_n est le quotient associé et l'on calcule $u_n = u_{n-2} - q_{n-1}u_{n-1}$ et $v_n = v_{n-2} - q_{n-1}v_{n-1}$.

q_i	r_i	u_i	v_i
	70	1	0
11	6	0	1
1	4	1	−11
2	2	−1	12
	0		

le pgcd

les coefs de Bézout

L'algorithme s'arrête au premier reste nul. Le pgcd est alors le dernier reste non nul et les coefficients de Bézout sont les nombres u_i et v_i de la ligne de ce reste.

Exemples :

- Pour 1658 et 156, on a

q_i	r_i	u_i	v_i
	1658	1	0
10	156	0	1
1	98	1	−10
1	58	−1	11
1	40	2	−21
2	18	−3	32
4	4	8	−85
2	2	−35	372
	0		

d'où

$1658 \wedge 156 = 2$

et

$2 = -35 \times 1658 + 372 \times 156.$

d) Entiers premiers entre eux

Définition 3

Les nombres entiers relatifs a et b sont dits premiers entre eux (ou étrangers) lorsque $a \wedge b = 1$, c'est-à-dire lorsque les seuls diviseurs communs de a et b sont 1 et -1.

Exemples :

- Deux entiers consécutifs sont toujours premiers entre eux. En effet, un diviseur commun à ces deux nombres divise leur différence, c'est-à-dire 1. Ce diviseur commun vaut donc ± 1.
- En divisant deux entiers a et b par leur pgcd, c'est-à-dire en considérant $a' = a/(a \wedge b)$ et $b' = b/(a \wedge b)$, on obtient deux entiers premiers entre eux, c'est-à-dire $a' \wedge b' = 1$.

La proposition ci-dessous donne une caractérisation très utile du pgcd, utilisant la notion d'entiers premiers entre eux.

Proposition 6

Soient $a, b \in \mathbb{Z}$. Un entier positif d est le pgcd de a et b si, et seulement si,

$$\exists a', b' \in \mathbb{Z}, \qquad a = a'd, \quad b = b'd \quad \text{et} \quad a' \wedge b' = 1.$$

■ On raisonne par double implication.

⇒ Supposons que $d = a \wedge b$. Comme d est un diviseur commun de a et b, il existe $a', b' \in \mathbb{Z}$ tels que $a = da'$ et $b = db'$. Alors, d'après la proposition 5, on a $a' \wedge b' = (a/d) \wedge (b/d) = (a \wedge b)/d = d/d = 1$.

⇐ Supposons réciproquement l'existence de $a', b' \in \mathbb{Z}$ tel que $a = a'd$, $b = b'd$ et $a' \wedge b' = 1$. Alors, toujours d'après la proposition 5, on a $a \wedge b = a'd \wedge b'd = d(a' \wedge b') = d \times 1 = d$. ■

Le théorème suivant, appelé théorème de Bézout, permet de caractériser simplement deux entiers premiers entre eux. Attribué à tort à Bézout, il est en fait dû à Bachet de Méziriac.

Théorème 2

Deux nombres entiers relatifs a et b sont premiers entre eux si, et seulement si, il existe $u, v \in \mathbb{Z}$ tels que $ua + vb = 1$.

■ Allons-y, montrons Bézout ! ;-)

⇒ Si a et b sont premiers entre eux, alors $a \wedge b = 1$ et l'on prend pour u et v les coefficients de Bézout fournis par la proposition 4.

⇐ S'il existe $u, v \in \mathbb{Z}$ tels que $ua + vb = 1$, alors, comme $a \wedge b$ divise $ua + vb$, on a $a \wedge b \mid 1$, ce qui donne $a \wedge b = 1$. Donc a et b sont premiers entre eux. ■

En général, l'égalité $ua + vb = d$ implique seulement que d est un multiple de $a \wedge b$. C'est seulement dans le cas où $d = 1$, que l'on peut affirmer que $a \wedge b = d = 1$.

Exemples :

- Pour tout $n \in \mathbb{Z}$, on a $1 \times (n+1) + (-1) \times n = 1$ donc n et $n+1$ sont premiers entre eux. On retrouve le fait que deux entiers consécutifs sont premiers entre eux.
- Soit $(F_n)_{n \geqslant 0}$ la suite de Fibonacci définie par $F_0 = 0$, $F_1 = 1$ et $\forall n \geqslant 0$, $F_{n+2} = F_{n+1} + F_n$. L'assertion $\forall n \geqslant 1$, $F_{n+1}F_{n-1} - {F_n}^2 = (-1)^n$ se démontre par récurrence. En interprétant cette égalité comme une relation de Bézout, on voit que $F_{n-1} \wedge F_n = 1$ pour tout $n \geqslant 1$. Deux termes consécutifs de la suite de Fibonacci sont donc toujours premiers entre eux.
- Les entiers d'un couple de Bézout sont toujours premiers entre eux. En effet, on peut réécrire l'égalité $ua + vb = a \wedge b$ sous la forme $u(a/a \wedge b) + v(b/a \wedge b) = 1$.

2 h 10

Le théorème de Bézout a beaucoup d'applications. Nous en proposons deux ci-dessous.

On commence par le lemme de Gauß, qui est si important qu'on l'énonce en tant que théorème.

Théorème 3

Soient $a, b, c \in \mathbb{Z}$. On a

$$\big(a \mid bc \quad \text{et} \quad a \wedge b = 1\big) \quad \Longrightarrow \quad (a \mid c).$$

■ Soient $a, b, c \in \mathbb{Z}$ tels que $a \wedge b = 1$ et $a \mid bc$. D'après le théorème de Bézout, il existe $u, v \in \mathbb{Z}$ tels que $ua + vb = 1$. En multipliant par c, on obtient $uac + vbc = c$. Le membre de gauche est alors clairement divisible par a. Il s'ensuit que le membre de droite aussi, c'est-à-dire $a \mid c$. ■

Le lemme de Gauß a de multiples applications. En voici une. Nous en verrons d'autres plus loin dans ce cours.

Corollaire 2

Tout nombre rationnel r s'écrit de manière unique sous la forme $r = a/b$ avec $a \in \mathbb{Z}$, $b \in \mathbb{N}^*$ et $a \wedge b = 1$. C'est l'écriture irréductible de r.

■ L'existence vient de la possibilité de simplifier numérateur et dénominateur d'une fraction par leur pgcd.

Pour l'unicité, on suppose que $a/b = a'/b'$ avec $a, a' \in \mathbb{Z}$, $b, b' \in \mathbb{N}^*$ et $a \wedge b = a' \wedge b' = 1$. Il s'ensuit que $ab' = a'b$, et donc $b' \mid a'b$ et $b \mid ab'$. Comme $a \wedge b = a' \wedge b' = 1$, le lemme de Gauß implique que $b' \mid b$ et $b \mid b'$. Par suite, on a $b = b'$ (car $b, b' \in \mathbb{N}$) puis $a = a'$. ■

La proposition suivante énonce la propriété d'indépendance divisorielle.

Proposition 7

Soient $a, b, c \in \mathbb{Z}$. On a

$$(a \mid c \quad \text{et} \quad b \mid c \quad \text{et} \quad a \wedge b = 1) \quad \Longrightarrow \quad (ab \mid c).$$

Autrement dit,

$$(a \wedge b = 1) \quad \Longrightarrow \quad (a\mathbb{Z} \cap b\mathbb{Z} = ab\mathbb{Z}).$$

■ Soient $a, b, c \in \mathbb{Z}$ tels que $a \wedge b = 1$, $a \mid c$ et $b \mid c$. D'après le théorème de Bézout, il existe $u, v \in \mathbb{Z}$ tels que $ua + vb = 1$. En multipliant par c, on obtient $uac + vbc = c$. Comme a et b divise c, il existe $q, q' \in \mathbb{Z}$ tels que $c = qa$ et $c = q'b$. En combinant ces égalités, on obtient $c = uaq'b + vbqa = (uq' + vq)ab$. On en déduit bien que $ab \mid c$. ■

Pourquoi appeler « indépendance divisorielle » cette propriété ?

Imaginons une probabilité sur $\mathbb{Z}$ qui serve à faire de l'arithmétique. Quelle serait naturellement la probabilité d'obtenir un nombre pair ? Clairement $1/2$. Et pour la probabilité d'obtenir un multiple de 3 ? Tout aussi clairement $1/3$. Plus généralement, une telle probabilité P devrait vérifier $P(a\mathbb{Z}) = 1/a$ pour tout $a \in \mathbb{N}^*$.

Dès lors, que pourait-on dire des événements $a\mathbb{Z}$ et $b\mathbb{Z}$ lorsque $a \wedge b = 1$? Et bien, d'après la proposition précédente, on aurait

$$P(a\mathbb{Z} \cap b\mathbb{Z}) = P(ab\mathbb{Z}) = \frac{1}{ab} = \frac{1}{a} \times \frac{1}{b} = P(a\mathbb{Z})P(b\mathbb{Z}),$$

ce qui voudrait dire que les événements $a\mathbb{Z}$ et $b\mathbb{Z}$ sont indépendants.

D'où le nom de cette propriété !

Seul « petit » grain de sable dans cette jolie explication : une telle probabilité, ça n'existe pas ! Ce qui n'a rien de trivial...

On termine avec la compatibilité du produit avec la relation « être premier avec ».

Proposition 8

Soient $a_1, \ldots, a_n \in \mathbb{Z}$ et $b \in \mathbb{Z}$. On a

$$(a_1 \wedge b = 1, \ldots, a_n \wedge b = 1) \quad \Longrightarrow \quad (a_1 \cdots a_n \wedge b = 1).$$

Autrement dit, si un nombre est premier avec des entiers, il est aussi premier avec le produit de ces entiers.

■ On traite le cas $n = 2$. Le cas général s'obtient ensuite par récurrence.

Soient $a_1, a_2, b \in \mathbb{Z}$ tels que $a_1 \wedge b = a_2 \wedge b = 1$. Par le théorème de Bézout, il existe $(u_1, v_1), (u_2, v_2) \in \mathbb{Z}^2$ tels que $u_1 a_1 + v_1 b = 1$ et $u_2 a_2 + v_2 b = 1$. Il s'ensuit que $(u_1 a_1 + v_1 b)(u_2 a_2 + v_2 b) = 1$, ce qui donne, après développement et regroupement, $(u_1 u_2) a_1 a_2 + (u_1 a_1 v_2 + v_1 u_2 a_2 + v_1 v_2 b) b = 1$. Le théorème de Bézout nous permet d'en déduire que $a_1 a_2 \wedge b = 1$. ■

Ce résultat nous servira à démontrer l'unicité de la décomposition en nombres premiers.

Exemples :

- Si a et b sont premiers entre-eux, alors pour tous $\alpha, \beta \in \mathbb{N}$, les entiers a^α et b^β sont également premiers entre eux.

e) Plus grand diviseur commun de plusieurs entiers

Définition 4

Soient $a_1, \dots, a_n \in \mathbb{Z}$. Le pgcd de $a_1, \dots, a_n$, noté $a_1 \wedge \cdots \wedge a_n$ ou $\text{pgcd}(a_1, \dots, a_n)$, est

(i) le plus grand des diviseurs communs à $a_1, \dots, a_n$ lorsque $(a_1, \dots, a_n) \neq (0, \dots, 0)$;

(ii) égal à 0 lorsque $a_1 = \cdots = a_n = 0$.

Comme dans le cas de deux entiers, le pgcd de plusieurs entiers est insensible aux signes des a_k puisque $a_1 \wedge \cdots \wedge a_n = |a_1| \wedge \cdots \wedge |a_n|$, ainsi qu'à l'ordre des a_k puisque, pour toute permutation σ de $[\![1; n]\!]$, on a $a_{\sigma(1)} \wedge \cdots \wedge a_{\sigma(n)} = a_1 \wedge \cdots \wedge a_n$.

Les propriétés suivantes généralisent celles du pgcd de deux entiers.

On commence par justifier que le pgcd est le plus grand diviseur au sens de la divisibilité.

Proposition 9

Soient $a_1, \dots, a_n \in \mathbb{Z}$. L'ensemble des diviseurs communs de $a_1, \dots, a_n$ est aussi l'ensemble des diviseurs du pgcd de $a_1, \dots, a_n$, c'est-à-dire

$$\mathscr{D}(a_1) \cap \cdots \cap \mathscr{D}(a_n) = \mathscr{D}(a_1 \wedge \cdots \wedge a_n).$$

■ On adapte la démonstration de la proposition 3. ■

On retiendra que

un entier d divise $a_1, \dots, a_n$ si, et seulement si, d divise $a_1 \wedge \cdots \wedge a_n$.

La notation $a_1 \wedge \cdots \wedge a_n$ ne fait pas apparaître de parenthèses, présupposant l'associativité de la loi $\wedge$. L'énoncé suivant valide cette écriture.

Proposition 10

Soient $a_1, \dots, a_n \in \mathbb{Z}$. La loi $\wedge$ est associative, c'est-à-dire

$$a_1 \wedge \cdots \wedge a_n = (a_1 \wedge \cdots \wedge a_{n-1}) \wedge a_n.$$

■ Cela découle de la proposition précédente. ■

Cette associativité est à la base du calcul du pgcd de plusieurs entiers : on applique itérativement l'algorithme d'Euclide à a_1 et a_2, puis à $a_1 \wedge a_2$ et a_3, etc.

On peut aussi introduire la notion de coefficients de Bézout.

Proposition 11

Soient $a_1, \dots, a_n \in \mathbb{Z}$. Il existe des entiers relatifs $u_1, \dots, u_n$, appelés coefficients de Bézout de $a_1, \dots, a_n$, tels que

$$u_1 a_1 + \cdots + u_n a_n = a_1 \wedge \cdots \wedge a_n.$$

Autrement dit,

$$a_1\mathbb{Z} + \cdots + a_n\mathbb{Z} = (a_1 \wedge \cdots \wedge a_n)\mathbb{Z}.$$

■ Par récurrence. ■

La technique décrite ci-dessus pour le calcul du pgcd permet aussi de déterminer les coefficients de Bézout de plusieurs entiers.

On peut alors généraliser la distributivité, dans $\mathbb{N}$, du produit sur le pgcd.

Proposition 12

Soient $k \in \mathbb{N}$ et $a_1, \dots, a_n \in \mathbb{Z}$. Alors

$$k(a_1 \wedge \cdots \wedge a_n) = ka_1 \wedge \cdots \wedge ka_n.$$

En particulier, si d est un diviseur strictement positif de $a_1, \dots, a_n$, on a

$$\frac{a_1}{d} \wedge \cdots \wedge \frac{a_n}{d} = \frac{a_1 \wedge \cdots \wedge a_n}{d}.$$

■ Par récurrence. ■

On peut aussi généraliser la notion d'entiers premiers entre eux.

Définition 5

Soient $a_1, \dots, a_n \in \mathbb{Z}$.

On dit que $a_1, \dots, a_n$ sont premiers entre eux deux à deux lorsque, pour tous $i, j \in [\![1; n]\!]$ avec $i \neq j$, on a $a_i \wedge a_j = 1$.

On dit que $a_1, \dots, a_n$ sont premiers entre eux dans leur ensemble lorsque $a_1 \wedge \cdots \wedge a_n = 1$, c'est-à-dire lorsque les seuls diviseurs communs de $a_1, \dots, a_n$ sont 1 et -1.

La notion d'« entiers premiers dans leur ensemble » est plus faible que celle d'« entiers premiers deux à deux ». Autrement dit, lorsque des entiers sont premiers entre eux deux à deux, alors ils sont premiers entre eux dans leur ensemble mais la réciproque est fausse. Par exemple, on a $6 \wedge 10 \wedge 15 = 1$ mais $6 \wedge 10 = 2$, $10 \wedge 15 = 5$ et $6 \wedge 15 = 3$.

Si l'on choisit $d = a_1 \wedge \cdots \wedge a_n$ (avec les a_k tous non nuls) dans la seconde formule de la proposition 12, on constate qu'en divisant $a_1, \dots, a_n$ par leur pgcd, on obtient des nombres premiers entre eux dans leur ensemble. Plus précisément, on a le résultat suivant.

Proposition 13

Soient $a_1, \dots, a_n \in \mathbb{Z}$. Un entier positif d est le pgcd de $a_1, \dots, a_n$ si, et seulement si,

$$\exists a'_1, \dots, a'_n \in \mathbb{Z}, \qquad a_1 = a'_1 d, \quad \dots, \quad a_n = a'_n d \quad \text{et} \quad a'_1 \wedge \cdots \wedge a'_n = 1.$$

■ Découle de la proposition 12. ■

Le théorème de Bézout se généralise au cas de plusieurs entiers.

Théorème 4

Une famille de nombres entiers relatifs $a_1, \dots, a_n$ sont premiers entre eux dans leur ensemble si, et seulement si, il existe $u_1, \dots, u_n \in \mathbb{Z}$ tel que $u_1 a_1 + \cdots + u_n a_n = 1$.

■ On adapte la démonstration vue dans le cas de deux entiers.

⇒ Si $a_1, \dots, a_n$ sont premiers entre eux dans leur ensemble, alors $a_1 \wedge \cdots \wedge a_n = 1$ et l'on prend pour $u_1, \dots, u_n$ les coefficients de Bézout fournis par la proposition 11.

⇐ S'il existe $u_1, \dots, u_n \in \mathbb{Z}$ tels que $u_1 a_1 + \cdots + u_n a_n = 1$, alors, comme $a_1 \wedge \cdots \wedge a_n$ divise la somme $u_1 a_1 + \cdots + u_n a_n$, on a $a_1 \wedge \cdots \wedge a_n \mid 1$, ce qui donne $a_1 \wedge \cdots \wedge a_n = 1$. Donc $a_1, \dots, a_n$ sont premiers entre eux dans leur ensemble. ■

En général, l'égalité $u_1 a_1 + \cdots + u_n a_n = d$ implique seulement que d est un multiple de $a_1 \wedge \cdots \wedge a_n$. C'est seulement dans le cas où $d = 1$, que l'on peut affirmer que $a_1 \wedge \cdots \wedge a_n = d = 1$.

Attention ! Pour généraliser la propriété d'indépendance divisorielle, l'hypothèse « premiers dans leur ensemble » ne suffit pas ! Il est nécessaire que les nombres soient premiers entre eux deux à deux.

Du coup, même si cette proposition est placée ici, elle n'est pas une conséquence du théorème de Bézout pour plusieurs entiers.

Proposition 14

Soient $a_1, \dots, a_n \in \mathbb{Z}$ et $c \in \mathbb{Z}$. On a l'indépendance divisorielle généralisée suivante :

$$(a_1 \mid c,\ \dots,\ a_n \mid c \quad \text{et} \quad a_1, \dots, a_n \text{ premiers entre eux deux à deux}) \implies (a_1 \cdots a_n \mid c).$$

Autrement dit,

$$(a_1, \dots, a_n \text{ premiers entre eux deux à deux}) \implies (a_1\mathbb{Z} \cap \cdots \cap a_n\mathbb{Z} = a_1 \cdots a_n\mathbb{Z}).$$

■ Par récurrence. ■

B. 2. Plus petit multiple commun

a) Plus petit multiple commun de deux entiers

Définition 6

Soient a et b deux nombres entiers relatifs. Le ppcm de a et b, noté $a \vee b$ ou $\text{ppcm}(a,b)$, est

(i) le plus petit des multiples strictement positifs communs à a et b lorsque $ab \neq 0$;

(ii) égal à 0 lorsque a ou b est nul.

■ Si $ab \neq 0$, l'ensemble des multiples strictement positifs communs à a et b est une partie de $\mathbb{N}$ non vide (puisqu'elle contient $|ab|$) et possède donc, à ce titre, un plus petit élément. ■

Notons que le ppcm est insensible aux signes de a et b puisque $a \vee b = |a| \vee |b|$ ainsi qu'à l'ordre de a et b puisque $a \vee b = b \vee a$. Par conséquent, on peut toujours supposer que $0 \leqslant b \leqslant a$.

Comme le pgcd, le ppcm est utile dans le calcul fractionnaire : il est le plus petit dénominateur commun de deux fractions que l'on veut mettre au même dénominateur pour les ajouter.

À ce stade, le ppcm est le plus petit multiple commun positif au sens de la relation d'ordre usuelle $\leqslant$ et non au sens de la divisibilité. Ainsi, si m est un multiple commun de a et b, on peut affirmer, pour l'instant, que $a \vee b \leqslant m$ mais pas encore que $a \vee b \mid m$.

Nous allons remédier à cela avec l'énoncé ci-dessous qui précise ce que donne l'intersection de deux ensembles de multiples, c'est-à-dire ce que vaut un ensemble de multiples communs.

Proposition 15

Soient $a, b \in \mathbb{Z}$. L'ensemble des multiples communs de a et b est aussi l'ensemble des multiples du ppcm de a et b, c'est-à-dire

$$a\mathbb{Z} \cap b\mathbb{Z} = (a \vee b)\mathbb{Z}.$$

■ Si $a = 0$ ou $b = 0$, c'est clair. Supposons dorénavant que $a \neq 0$ et $b \neq 0$.

Les ensembles $a\mathbb{Z}$ et $b\mathbb{Z}$ sont des sous-groupes de $\mathbb{Z}$ donc $a\mathbb{Z} \cap b\mathbb{Z}$ est aussi un sous-groupe de $\mathbb{Z}$ (en tant qu'intersection de sous-groupes). Par conséquent, il existe $m \in \mathbb{N}^*$ tel que $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$. Dès lors, le plus petit élément strictement positif de $a\mathbb{Z} \cap b\mathbb{Z}$ est égal au plus petit élément strictement positif de $m\mathbb{Z}$, c'est-à-dire $a \vee b = m$. D'où le résultat. ■

Ce résultat signifie que $a \vee b$ est le plus petit, au sens de la divisibilité, des multiples positifs communs à a et b.(†)

C'est même valable si $a = 0$ ou $b = 0$ car dans ce cas, l'ensemble des multiples positifs communs est $\{0\}$ et 0 est bien le plus petit élément de $\{0\}$ pour la divisibilité.

On retiendra que

> un entier m est multiple de a et b si, et seulement si, m est multiple de $a \vee b$.

On utilise quelquefois ce résultat pour déterminer le ppcm de deux entiers a et b lorsque l'on connait un candidat potentiel pour le rôle. Pour cela, on montre que ce candidat μ est un multiple de a et b puis que tout multiple m de a et b est un multiple de μ.

(†) Pour la relation de divisibilité, un majorant est un multiple. Par conséquent, $a \vee b$ est le plus petit des majorants de $\{a; b\}$, c'est-à-dire que $a \vee b$ est la borne supérieure de $\{a; b\}$.

La proposition 15 permet aussi d'établir la distributivité, dans $\mathbb{N}$, du produit sur le ppcm.

Proposition 16

Soient $k \in \mathbb{N}$ et $a, b \in \mathbb{Z}$. On a

$$k(a \vee b) = ka \vee kb.$$

En particulier, si d est un diviseur strictement positif de a et b, on a

$$\frac{a}{d} \vee \frac{b}{d} = \frac{a \vee b}{d}.$$

4 h 00

■ On a $k(a \vee b)\mathbb{Z} = k(a\mathbb{Z} \cap b\mathbb{Z}) = (ka)\mathbb{Z} \cap (kb)\mathbb{Z} = (ka \vee kb)\mathbb{Z}$, d'où $ka \vee kb = k(a \vee b)$. ■

b) Plus petit multiple commun de plusieurs entiers

Définition 7

Soient $a_1, \dots, a_n \in \mathbb{Z}$. Le ppcm de $a_1, \dots, a_n$, noté $a_1 \vee \cdots \vee a_n$ ou $\mathrm{ppcm}(a_1, \dots, a_n)$, est

(i) le plus petit, dans $\mathbb{N}^*$, des multiples communs à $a_1, \dots, a_n$ lorsque $a_1 \cdots a_n \neq 0$;

(ii) 0 lorsque a_1 ou a_2 ou … ou a_n est nul.

Comme dans le cas de deux entiers, le ppcm de plusieurs entiers est insensible aux signes des a_k puisque $a_1 \vee \cdots \vee a_n = |a_1| \vee \cdots \vee |a_n|$, ainsi qu'à l'ordre des a_k puisque, pour toute permutation σ de $[\![1; n]\!]$, on a $a_{\sigma(1)} \vee \cdots \vee a_{\sigma(n)} = a_1 \vee \cdots \vee a_n$.

Le ppcm de plusieurs entiers est le plus petit dénominateur commun de plusieurs fractions que l'on veut mettre au même dénominateur pour les ajouter.

Les propriétés suivantes généralisent celles du ppcm de deux entiers.

On commence par justifier que le ppcm est le plus petit diviseur au sens de la divisibilité.

Proposition 17

Soient $a_1, \dots, a_n \in \mathbb{Z}$. L'ensemble des multiples communs de $a_1, \dots, a_n$ est aussi l'ensemble des multiples du ppcm de $a_1, \dots, a_n$, c'est-à-dire

$$a_1\mathbb{Z} \cap \cdots \cap a_n\mathbb{Z} = (a_1 \vee \cdots \vee a_n)\mathbb{Z}.$$

■ On adapte la démonstration de la proposition 15. ■

On retiendra que

un entier m est multiple de $a_1, \dots, a_n$ si, et seulement si, m est multiple de $a_1 \vee \cdots \vee a_n$.

La notation $a_1 \vee \cdots \vee a_n$ ne fait pas apparaître de parenthèses, présupposant l'associativité de la loi $\vee$. L'énoncé suivant valide cette écriture.

Proposition 18

Soient $a_1, \dots, a_n \in \mathbb{Z}$. La loi $\vee$ est associative, c'est-à-dire

$$a_1 \vee \cdots \vee a_n = (a_1 \vee \cdots \vee a_{n-1}) \vee a_n.$$

■ Cela découle de la proposition précédente. ■

On peut alors généraliser la distributivité, dans $\mathbb{N}$, du produit sur le ppcm.

Proposition 19

Soient $k \in \mathbb{N}$ et $a_1, \dots, a_n \in \mathbb{Z}$. On a

$$k(a_1 \vee \cdots \vee a_n) = ka_1 \vee \cdots \vee ka_n.$$

En particulier, si d est un diviseur strictement positif de $a_1, \dots, a_n$, on a

$$\frac{a_1}{d} \vee \cdots \vee \frac{a_n}{d} = \frac{a_1 \vee \cdots \vee a_n}{d}.$$

■ Par récurrence. ■

B.3. Lien entre le pgcd et le ppcm

Commençons par un lemme donnant le ppcm de deux entiers premiers entre eux.

Lemme 2

Soient a, b deux entiers relatifs premiers entre eux. Alors $a \vee b = |ab|$.

■ Comme $a \wedge b = 1$, la propriété d'indépendance divisorielle nous dit que $a\mathbb{Z} \cap b\mathbb{Z} = (ab)\mathbb{Z}$. Par ailleurs, on a vu, à la proposition 15, que $a\mathbb{Z} \cap b\mathbb{Z} = (a \vee b)\mathbb{Z}$. On a donc $(ab)\mathbb{Z} = (a \vee b)\mathbb{Z}$, ce qui donne $|ab| = a \vee b$. ■

On peut alors énoncer la formule liant le pgcd et le ppcm de deux entiers.

Proposition 20

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

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

■ Posons $\delta = a \wedge b$ et $\mu = a \vee b$. On sait qu'il existe $a', b' \in \mathbb{Z}$ tel que $a' \wedge b' = 1$, $a = \delta a'$ et $b = \delta b'$. Alors $\mu = \delta a' \vee \delta b' = \delta \times (a' \vee b') = \delta |a'b'|$ d'après le lemme précédent. Donc $\delta\mu = |\delta a' \delta b'| = |ab|$, c'est-à-dire $(a \wedge b) \times (a \vee b) = |ab|$. ■

On peut retenir de cet énoncé que le calcul effectif du ppcm de deux entiers se ramène au calcul du pgcd d'iceux (qui se fait par l'algorithme d'Euclide).

Attention ! La formule $(a \wedge b) \times (a \vee b) = |ab|$ ne se généralise pas à plus de trois entiers. Par exemple, on a $(6 \wedge 10 \wedge 15) \times (6 \vee 10 \vee 15) = 1 \times 30 \neq 6 \times 10 \times 15$.

Du coup, pour calculer le ppcm de plusieurs entiers, on utilise, comme pour le pgcd, l'associativité pour se ramener à des calculs successifs de ppcm de deux entiers.

B.4. Résolution de l'équation diophantienne linéaire binaire [✠]

Équation diophantienne

Soient a, b, c trois entiers relatifs avec $a \neq 0$ et $b \neq 0$. On se propose de résoudre l'équation d'inconnue $(x; y) \in \mathbb{Z}^2$ suivante :

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

▶ *Existence ou non de solutions*

On commence par effectuer l'algorithme d'Euclide pour déterminer $\delta = a \wedge b$.

Si c n'est pas un multiple de $a \wedge b$, l'équation (E) n'admet pas de solution, car pour tout $(x, y) \in \mathbb{Z}^2$, $ax + by$ est un multiple de $a \wedge b$.

Si c est un multiple de $\delta = a \wedge b$, nous allons voir que l'équation (E) admet une infinité de solutions $(x, y) \in \mathbb{Z}^2$ et nous allons apprendre à les déterminer.

▶ *Détermination de l'ensemble des solutions dans le cas où $\delta \,|\, c$*

▷ Recherche d'une solution particulière

Pour cela, on écrit $a = \delta a'$, $b = \delta b'$ avec $a' \wedge b' = 1$ et $c = \delta c'$, de sorte que (E) est équivalente à

$$(E) \qquad a'x + b'y = c' \qquad \text{avec } a' \wedge b' = 1.$$

On recherche alors, à l'aide de l'algorithme d'Euclide, un couple de coefficients de Bézout $(u', v') \in \mathbb{Z}^2$ tel que $a'u' + b'v' = 1$, de sorte que, si l'on pose $x_0 = c'u'$ et $y_0 = c'v'$, on a $a'x_0 + b'y_0 = c'$. Autrement dit, (x_0, y_0) est une solution particulière de (E).

▷ Ensemble des solutions

Soit $(x, y) \in \mathbb{Z}^2$ une solution de (E).
Comme $a'x_0 + b'y_0 = c'$, l'équation (E) est équivalente à $a'x + b'y = a'x_0 + b'y_0$, c'est-à-dire à $a'(x - x_0) = b'(y_0 - y)$. Il s'ensuit que b' divise $a'(x - x_0)$. Mais, comme $a' \wedge b' = 1$, le lemme de Gauß permet d'en déduire que b' divise $x - x_0$, ce qui peut s'écrire $x = x_0 + kb'$ avec $k' \in \mathbb{Z}$.
En réinjectant dans l'équation (E), on en déduit que $y = y_0 - ka'$.
On constate alors que $(x_0 + kb', y_0 - ka')$ est bien un couple de solutions de (E).

▷ Bilan

L'ensemble $\mathscr{S}$ des solutions de (E) est

$$\boxed{\mathscr{S} = \{(x_0 + kb', y_0 - ka') : k \in \mathbb{Z}\}.}$$

Exemples :

- Résolvons $12x + 3y = 15$.
  Comme $12 \wedge 3 = 3$, on divise l'équation par 3 pour obtenir $4x + y = 5$.
  Le couple $(1, 1)$ est une solution évidente.
  L'ensemble des solutions est $(1 + k, 1 - 4k)$ où $k \in \mathbb{Z}$.

C. Nombres premiers

C.1. Définition et premières propriétés des nombres premiers

Définition 8

Un nombre premier (ou nombre irréductible) est un entier naturel qui admet exactement deux diviseurs positifs distincts : 1 et lui-même. En particulier, 1 n'est pas un nombre premier puisqu'il ne possède qu'un seul diviseur positif.

L'ensemble des nombres premiers est noté $\mathbb{P}$.

Un nombre est donc premier s'il représente le nombre d'élèves d'une classe avec laquelle un professeur de sport ne peut pas faire plusieurs équipes de même taille.

Exemples :

- 2 est le seul nombre premier pair (« 2 is the oddest prime number »).
- Voici une liste des premiers nombres premiers : 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, ...

La proposition suivante rassemble les premières propriétés des nombres premiers.

Proposition 21

Soit $p \in \mathbb{N} \setminus \{0; 1\}$. Il est équivalent de dire :

(i) p est un nombre premier ;

(ii) p est premier avec tout entier qu'il ne divise pas ;

(iii) p est premier avec tout nombre premier contenu dans $[1, \sqrt{p}]$.

■ On va démontrer que (i) $\Longrightarrow$ (ii) $\Longrightarrow$ (iii) $\Longrightarrow$ (i).

(i)⇒(ii) On suppose que p est premier. Soit n un entier tel que p ne divise pas n. On veut montrer que $n \wedge p = 1$. On sait que $n \wedge p$ divise p. Comme p est premier, cela laisse comme seules possibilités, $n \wedge p = 1$ ou $n \wedge p = p$. Mais p ne divisant pas n, la seconde alternative est impossible, donc $n \wedge p = 1$.

(ii)⇒(iii) C'est clair puisque tout multiple de p est strictement supérieur à $\sqrt{p}$.

(iii)⇒(i) Supposons que p est premier avec tout nombre premier de $[1, \sqrt{p}]$ et déduisons-en que p est lui-même premier. On raisonne par l'absurde en supposant que p n'est pas premier. Considérons alors q le plus petit diviseur de p différent de 1. C'est nécessairement un nombre premier (sinon il possèderait un diviseur strictement compris entre 1 et q qui serait aussi un diviseur de p, ce qui contredirait la minimalité de q). De plus, on peut affirmer que $q \in [1, \sqrt{p}]$ sinon p/q serait un diviseur de p plus petit que q et différent de 1 (puisque $q \neq p$), ce qui contredirait là encore la minimalité de q. D'après (iii), on a alors $p \wedge q = 1$. Or $p \wedge q = q$ puisque $q \mid p$. Donc $q = 1$. C'est absurde ! Ainsi p est bien un nombre premier. ■

L'implication (i) $\Longrightarrow$ (ii) dit, en particulier, qu'un nombre premier est premier avec tous les entiers naturels (non nuls) qui le précèdent mais aussi avec tous les autres nombres premiers.

L'équivalence entre (i) et (iii) s'appelle le crible d'Ératosthène.

Ce crible permet d'établir la liste des nombres premiers inférieurs à un seuil donné n. Il suffit pour cela d'éliminer les multiples de 2 inférieurs à n, puis ceux de 3, puis ceux de 5, ainsi de suite jusqu'au dernier nombre premier inférieur ou égal à $\sqrt{n}$.

Dans le cas $n = 49$, on trouve :

	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~~

La répartition des nombres premiers au sein des entiers naturels est une question centrale de la théorie des nombres qui remonte au théorème d'Euclide (III-ème av. J.-C.) énonçant que $\mathbb{P}$ est un ensemble infini.

Théorème 5

Il existe une infinité de nombres premiers.

■ Raisonnons par l'absurde en supposant qu'il existe un nombre fini de nombres premiers. Notons alors $p_1, \dots, p_n$ la liste exhaustive de tous les nombres premiers et posons $N = p_1 p_2 \cdots p_n - 1$.

Comme $p_1 = 2$ et $p_2 = 3, \dots$ on sait que $N \geqslant 2$. Le nombre N possède donc nécessairement un diviseur premier q. Il suffit en effet de prendre pour q le plus petit diviseur de N différent de 1. Ce nombre q est nécessairement un nombre premier, sinon il possèderait lui-même un diviseur strictement compris entre 1 et q, qui serait alors aussi un diviseur de N, contredisant ainsi la minimalité de q.

Dès lors, q fait partie des nombres premiers $p_1, \dots, p_n$, ce qui prouve qu'il divise $N + 1$. Comme q divise N et $N + 1$, il divise leur différence, c'est-à-dire 1. C'est absurde pour un nombre premier. ■

Affirmer qu'il existe des nombres premiers aussi grands qu'on le souhaite est une chose. C'en est une autre de trouver de « grands » nombres premiers...

À bien y regarder, la démonstration du théorème d'Euclide permet de donner une majoration de la taille du n-ème nombre premier p_n. En effet, le raisonnement tenu ci-dessus implique que, pour tout $n \in \mathbb{N}^*$, on a $p_{n+1} < p_1 \cdots p_n$. Une récurrence forte permet d'en déduire immédiatement que $p_n \leqslant 2^{2^n}$ pour tout $n \geqslant 1$. Il n'est alors pas très difficile de voir que, si $\pi(n)$ désigne le nombre de nombres premiers inférieurs ou égaux à n, on a $\forall n \geqslant 2,\ \pi(n) \geqslant \ln(\ln n)$.

Ces estimations sont loin d'être optimales. Le théorème des nombres premiers, démontré en 1896 par Hadamard et de la Vallée Poussin, énonce que

$$\pi(n) \underset{n \to +\infty}{\sim} \frac{n}{\ln n},$$

ce qui a pour corollaire que

$$p_n \underset{n \to +\infty}{\sim} n \ln n.$$

C.2. Décomposition primaire

Le théorème suivant permet d'interpréter les nombres premiers comme les atomes constituant les molécules que sont les entiers naturels.

Théorème 6

Tout nombre entier naturel n supérieur ou égal à 2 admet une décomposition en facteurs premiers unique à l'ordre des facteurs près. Autrement dit,

(i) pour tout entier $n \geqslant 2$, il existe une famille $p_1, \dots, p_r$ de nombres premiers distincts tels que $n = {p_1}^{\alpha_1} \cdots {p_r}^{\alpha_r}$ où $\alpha_1, \dots, \alpha_r \in \mathbb{N}^*$;

(ii) cette décomposition est unique à l'ordre près des facteurs.

Cette propriété s'étend aux entiers relatifs à condition d'attribuer un signe à cette décomposition. Elle fait de $(\mathbb{Z}, +, \times)$ un anneau dit factoriel.

■ ▶ Démontrons l'existence par récurrence forte. Pour tout $n \geqslant 2$, on note $\mathscr{P}_n$ l'assertion « tout nombre entier compris entre 2 et n admet une décomposition en facteurs premiers ».

Initialisation : La propriété $\mathscr{P}_2$ est vérifiée car 2 est un nombre premier.

Hérédité : Fixons $n \geqslant 3$ tel que $\mathscr{P}_{n-1}$ est vraie et démontrons que n admet une décomposition en facteurs premiers, ce qui prouvera $\mathscr{P}_n$. On distingue deux cas :

▷ Si n est un nombre premier alors c'est un produit d'un seul nombre premier.

▷ Sinon, n admet un diviseur premier p (on a déjà vu pourquoi : il suffit de prendre le plus petit diviseur de n strictement supérieur à 1). Le nombre n/p, qui est strictement inférieur à n, peut alors être décomposé en facteurs premiers (par H.R.), d'où l'existence de nombres premiers $p_1, \dots, p_r$ tels que $n/p = {p_1}^{\alpha_1} \cdots {p_r}^{\alpha_r}$. Cela fournit la décomposition de n en facteurs premiers : $n = p \times {p_1}^{\alpha_1} \cdots {p_r}^{\alpha_r}$.

Donc $\mathscr{P}_n$ est vraie.

Conclusion : D'après le principe de récurrence, $\mathscr{P}_n$ est vraie pour tout $n \geqslant 2$, ce qui justifie l'existence de la décomposition en nombres premiers.

▶ Démontrons ensuite l'unicité d'une telle décomposition. Supposons qu'un entier $n \geqslant 2$ admette deux décompositions $n = {p_1}^{\alpha_1} \cdots {p_r}^{\alpha_r}$ et $n = {p_1}^{\beta_1} \cdots {p_r}^{\beta_r}$ où $r \in \mathbb{N}^*$, $p_1, \dots, p_r$ sont des nombres premiers deux à deux distincts et $\alpha_1, \dots, \alpha_r, \beta_1, \dots, \beta_r \in \mathbb{N}$. On peut bien considérer que les décompositions contiennent les mêmes nombres premiers puisqu'on a supposé que les exposants α_i et β_i peuvent être nuls (donc si un nombre premier est dans l'une des décompositions et pas dans l'autre, on le rajoute avec un exposant nul, là où il manque).
Raisonnons alors par l'absurde en supposant qu'il existe $k \in [\![1; r]\!]$ tel que $\alpha_k \neq \beta_k$, par exemple $\alpha_k < \beta_k$. En simplifiant l'égalité ${p_1}^{\alpha_1} \cdots {p_r}^{\alpha_r} = {p_1}^{\beta_1} \cdots {p_r}^{\beta_r}$ par ${p_k}^{\alpha_k}$, on voit qu'il reste un facteur ${p_k}^{\beta_k - \alpha_k}$ à droite, ce qui implique que le membre de gauche est divisible par p_k, c'est-à-dire

$$p_k \mid \prod_{\substack{j=1 \\ j \neq k}}^{r} {p_j}^{\alpha_j}.$$

Or, lorsque $j \neq k$, les nombres premiers p_k et p_j sont distincts donc premiers entre eux. D'après la proposition 8, on a donc

$$p_k \wedge \prod_{\substack{j=1 \\ j \neq k}}^{r} {p_j}^{\alpha_j} = 1.$$

Il s'ensuit que $p_k = 1$, ce qui est absurde !
Par suite, on a $\forall i \in [\![1; r]\!]$, $\alpha_i = \beta_i$, ce qui démontre l'unicité de la décomposition. ■

Décomposer un entier en facteurs premiers est une opération difficile même pour un ordinateur puissant. C'est sur cette idée que repose le système de codage RSA (Rivest, Shamir et Adleman).

Exemples :

- On a $272\,569 = 11 \times 71 \times 349$.

Donnons immédiatement une première application de la décomposition primaire. En général, lorsque $c \mid ab$, on ne peut pas en déduire que $c \mid a$ ou $c \mid b$. Ainsi 6 divise 4×9 mais 6 ne divise ni 4 ni 9. En revanche, dans le cas d'un nombre premier, la propriété suivante dit que c'est vrai.

Proposition 22

Soient $a, b \in \mathbb{Z}$ et $p \in \mathbb{N}$. On a

$$(p \text{ premier} \quad \text{et} \quad p \mid ab) \quad \Longrightarrow \quad (p \mid a \quad \text{ou} \quad p \mid b).$$

Ainsi, un nombre premier divise un produit si, et seulement si, il divise l'un de ses facteurs.

■ Les cas où a ou b appartiennent à $\{-1; 0; 1\}$ sont évidents. Sinon, si un nombre premier p divise ab, c'est qu'il est dans la décomposition primaire de ab et donc qu'il est nécessairement aussi dans la décomposition primaire de a ou dans celle de b, ce qui signifie bien que p divise a ou b. ■

Le fait qu'un nombre premier p puisse apparaître plusieurs fois dans la décomposition d'un entier motive la définition suivante.

Définition 9

Soit $n \in \mathbb{Z}^*$. L'exposant d'un nombre premier p dans la décomposition en facteurs premiers d'un entier n s'appelle la valuation p-adique de p dans n et est notée $v_p(n)$. On a donc $v_p(n) = 0$ lorsque p ne divise pas n. Autrement dit, $p^{v_p(n)}$ est la plus grande puissance de p qui divise n.

On peut alors écrire

$$n = \pm \prod_{p \in \mathbb{P}} p^{v_p(n)}.$$

Pour tout $p \in \mathbb{P}$, on a $v_p(\pm 1) = 0$.

La valuation est une fonction « logarithmique », comme le justifie la proposition suivante.

Proposition 23

Pour tout $p \in \mathbb{P}$ et tous $a, b, d \in \mathbb{Z}^*$ avec d qui divise a, on a

$$v_p(ab) = v_p(a) + v_p(b) \qquad \text{et} \qquad v_p\Big(\frac{a}{d}\Big) = v_p(a) - v_p(d).$$

■ Comme $p^{v_p(a)}$ est la plus grande puissance de p qui divise a et comme $p^{v_p(b)}$ est la plus grande puissance de p qui divise b, le nombre $p^{v_p(a)}p^{v_p(b)} = p^{v_p(a)+v_p(b)}$ est la plus grande puissance de p qui divise ab, ce qui démontre la première des deux formules. La seconde en découle. ■

On peut caractériser la divisibilité à l'aide des valuations.

Proposition 24

Soient $a, b \in \mathbb{Z}^*$. Alors b divise a si, et seulement si, $v_p(b) \leqslant v_p(a)$ pour tout $p \in \mathbb{P}$.

■ On raisonne par double implication.

⇒ Supposons que b divise a de sorte qu'il existe $q \in \mathbb{Z}$ tel que $a = bq$. Alors, pour tout $p \in \mathbb{P}$, on a $v_p(a) = v_p(bq) = v_p(b) + v_p(q) \geqslant v_p(b)$ où la deuxième égalité découle de la proposition 23.

⇐ Supposons que $v_p(b) \leqslant v_p(a)$ pour tout $p \in \mathbb{P}$. Alors, on a

$$a = \pm \prod_{p \in \mathbb{P}} p^{v_p(a)} = \pm \prod_{p \in \mathbb{P}} p^{v_p(b)} \times \prod_{p \in \mathbb{P}} p^{v_p(a)-v_p(b)} = b \times \Big(\pm \prod_{p \in \mathbb{P}} p^{v_p(a)-v_p(b)} \Big),$$

ce qui démontre que b divise a. ■

La décomposition en nombres premiers permet également de calculer le pgcd et le ppcm de deux entiers.

Proposition 25

Soient $a, b \in \mathbb{Z} \setminus \{-1; 0; 1\}$. On a

$$a \wedge b = \prod_{p \in \mathbb{P}} p^{\min\{v_p(a), v_p(b)\}} \qquad \text{et} \qquad a \vee b = \prod_{p \in \mathbb{P}} p^{\max\{v_p(a), v_p(b)\}}.$$

■ Un diviseur commun d de a et b est tel que, pour tout $p \in \mathbb{P}$, on a $v_p(d) \leqslant v_p(a)$ et $v_p(d) \leqslant v_p(b)$, c'est-à-dire $\forall p \in \mathbb{P},\ v_p(d) \leqslant \min\{v_p(a), v_p(b)\}$. Le plus grand des diviseurs communs à a et b est donc obtenu lorsque $\forall p \in \mathbb{P},\ v_p(d) = \min\{v_p(a), v_p(b)\}$, ce qui démontre la première égalité.

Un multiple commun m de a et b est tel que, pour tout $p \in \mathbb{P}$, on a $v_p(m) \geqslant v_p(a)$ et $v_p(m) \geqslant v_p(b)$, c'est-à-dire $\forall p \in \mathbb{P},\ v_p(m) \geqslant \max\{v_p(a), v_p(b)\}$. Le plus petit des multiples communs à a et b est donc obtenu lorsque $\forall p \in \mathbb{P},\ v_p(m) = \max\{v_p(a), v_p(b)\}$, ce qui démontre la seconde égalité. ■

Il est important de noter que cette technique de calcul du pgcd et du ppcm ne fonctionne que pour des entiers assez petits. Pour de grands entiers, la décomposition en nombres premiers est beaucoup trop longue à effectuer (même avec une machine) pour que ce calcul soit possible. Il est alors nettement plus efficace de se rabattre sur l'algorithme d'Euclide.

Exemples :

- Calculons le pgcd et le ppcm de 1 836 et 234.

  On commence par déterminer la décomposition de 1 836 et 234 en facteurs premiers, ce qui donne

1 836	2			234	2
918	2			117	3
459	3			39	3
153	3		et	13	13
51	3			1	
17	17				
1					

  c'est-à-dire

$$1\,836 = 2^2 \times 3^3 \times 17 \qquad \text{et} \qquad 234 = 2 \times 3^2 \times 13.$$

  Pour le pgcd, il suffit alors de prendre tous les facteurs premiers qui apparaissent simultanément dans les deux décompositions est les affectant de la plus petite puissance rencontrée dans ces mêmes décompositions, ce qui donne

$$1\,836 \wedge 234 = 2 \times 3^2 = 18.$$

  Pour le ppcm, on prend tous les facteurs premiers qui apparaissent dans l'une ou l'autre des deux décompositions et on leur affecte la plus grande puissance rencontrée dans ces mêmes décompositions. Ici, cela donne :

$$1\,836 \vee 234 = 2^2 \times 3^3 \times 13 \times 17 = 23\,868.$$

  On vérifie bien que

$$(1\,836 \wedge 234) \times (1\,836 \vee 234) = 18 \times 23\,868 = 429\,624 = 1\,836 \times 234.$$

5 h 50

D. Congruences

D.1. Définition et premières propriétés des congruences

On introduit ici la relation de modularité, notion indissociable de la division euclidienne.

Définition 10

Soient $n \in \mathbb{N}^*$ et $a, b \in \mathbb{Z}$. On dit que a et b sont congrus modulo n (ou encore que a est congru à b modulo n) lorsque n divise $a - b$, c'est-à-dire lorsqu'il existe $k \in \mathbb{Z}$ tel que $a = b + kn$. Dans ce cas, on note $a \equiv b\ [n]$ ou $a \equiv b\ (\mathrm{mod}\, n)$.

Le théorème de la division euclidienne se reformule ainsi : « Tout entier relatif a est congru modulo n à un entier r compris dans $[\![0; n-1]\!]$ ».

La congruence de a et b modulo n exprime que ces deux nombres ont le même reste dans la division euclidienne par n.

Écrire que $a \equiv 0\ [n]$ revient à dire que $n \mid a$. La relation de « congruence à 0 » n'est donc rien d'autre que la divisibilité.

Exemples :

- Deux nombres de même parité sont congrus modulo 2.
- $365 \equiv 1\ [7]$. C'est ce qui explique l'avancée d'un jour dans la semaine d'une date donnée lorsqu'on passe d'une année à l'année suivante (si les deux années ne sont pas bissextiles).
- Pour dire que $n \in \mathbb{N}$ s'écrit en nombre décimal à l'aide des chiffres c_0 (unités), c_1 (dizaines), c_2 (centaines), …, c_r où $r \in \mathbb{N}^*$, on utilise la notation $n = \overline{c_r \cdots c_1 c_0}$, avec $c_k \in [\![0; 9]\!]$ pour tout $k \in [\![1; r]\!]$ et $c_r \neq 0$. Cela signifie en fait que $n = c_0 \times 10^0 + c_1 \times 10^1 + \cdots + c_r \times 10^r$. Or, pour tout $k \in \mathbb{N}$, la formule de Bernoulli (i.e. la factorisation de $a^n - b^n$) dit que l'on peut factoriser $10 - 1 = 9$ dans l'expression $10^k - 1$, autrement dit que $9 \mid 10^k - 1$. Il s'ensuit que $n - (c_0 + c_1 + \cdots + c_r) = c_0 \times (10^0 - 1) + c_1 \times (10^1 - 1) + \cdots + c_r \times (10^r - 1)$ est nécessairement divisible par 9 ou encore que

$$\overline{c_r \cdots c_1 c_0} \equiv c_0 + c_1 + \cdots + c_r \quad [9],$$

  ce qui signifie que tout entier naturel est congru modulo 9 à la somme de ses chiffres. Nous verrons que c'est cette remarque qui fonde le principe de la preuve par 9.

Nous allons voir qu'en calcul modulaire, la congruence joue le rôle de l'égalité. On peut d'ores et déjà dire qu'elles ont en commun le fait d'être des relations d'équivalence.

Proposition 26

Soit $n \in \mathbb{N}^*$. La congruence modulo n est une relation d'équivalence :

(i) $\forall a \in \mathbb{Z},\quad a \equiv a\ [n]$ (réflexivité) ;

(ii) $\forall a, b \in \mathbb{Z},\quad \big(a \equiv b\ [n]\big) \iff \big(b \equiv a\ [n]\big)$ (symétrie) ;

(iii) $\forall a, b, c \in \mathbb{Z},\quad \big(a \equiv b\ [n] \text{ et } b \equiv c\ [n]\big) \implies \big(a \equiv c\ [n]\big)$ (transitivité).

■ (i) Soit $a \in \mathbb{Z}$. On a $n \mid a - a$ puisque 0 est divisible par tout autre nombre entier. Donc $a \equiv a\ [n]$.

(ii) Soient $a, b \in \mathbb{Z}$ tels que $a \equiv b\ [n]$. Alors $n \mid a - b$ et donc aussi $n \mid b - a$, ce qui donne $b \equiv a\ [n]$.

(iii) Soient $a, b, c \in \mathbb{Z}$ tels que $a \equiv b\ [n]$ et $b \equiv c\ [n]$. Alors $n \mid a - b$ et $n \mid b - c$, donc $n \mid (a - b) + (b - c)$, c'est-à-dire $n \mid a - c$. Donc $a \equiv c\ [n]$. ■

C'est la propriété de symétrie qui justifie que l'on puisse dire indifféremment que « a est congru à b modulo n », que « b est congru à a modulo n » ou même que « a et b sont congrus modulo n ».

La proposition suivante justifie tout l'intérêt de la notion de congruence.

Proposition 27

Soit $n \in \mathbb{N}^*$. La congruence modulo n est compatible avec $+$ et $\times$, c'est-à-dire

(i) $\forall a, b, c, d \in \mathbb{Z}, \quad \big(a \equiv b\ [n] \text{ et } c \equiv d\ [n]\big) \Longrightarrow \big(a + c \equiv b + d\ [n]\big)$;

(ii) $\forall a, b, c, d \in \mathbb{Z}, \quad \big(a \equiv b\ [n] \text{ et } c \equiv d\ [n]\big) \Longrightarrow \big(ac \equiv bd\ [n]\big)$;

(iii) $\forall a, b, \in \mathbb{Z},\ \forall m \in \mathbb{N}^*, \quad \big(a \equiv b\ [n]\big) \Longrightarrow \big(am \equiv bm\ [nm]\big)$.

En particulier, la propriété (ii) nous dit que

(ii)' $\forall a, b \in \mathbb{Z},\ \forall p \in \mathbb{N}, \quad \big(a \equiv b\ [n]\big) \Longrightarrow \big(a^p \equiv b^p\ [n]\big)$.

■ Soient $a, b, c, d \in \mathbb{Z}$ et $m \in \mathbb{N}^*$.

(i) On suppose que $a \equiv b\ [n]$ et $c \equiv d\ [n]$, c'est-à-dire n divise $a - b$ et $c - d$. Alors n divise la somme $(a - b) + (c - d) = (a + c) - (b - d)$, ce qui donne $a + c \equiv b + d\ [n]$.

(ii) On suppose que $a \equiv b\ [n]$ et $c \equiv d\ [n]$, c'est-à-dire n divise $a-b$ et $c-d$. Alors n divise la combinaison $(a - b)c + (c - d)b = ac - bd$ (Binet n'est pas loin !), ce qui donne $ac \equiv bd\ [n]$.

(iii) On suppose que $a \equiv b\ [n]$, c'est-à-dire n divise $a - b$. Alors nm divise $m(a - b)$, ce qui donne $am \equiv bm\ [nm]$. ■

Ne confondez pas les propriétés (ii) et (iii). Dans (ii), on fait le produit de deux égalités modulaires : le modulo n'est pas modifié. Dans (iii), on « dilate » une égalité modulaire par un entier m : tout est multiplié par m, le modulo y compris !

Les règles opératoires énoncées dans la proposition précédente permettent de mener les calculs modulo n de manière efficace. Elles expliquent en particulier que, dans un calcul avec des produits et des sommes, mieux vaut réduire modulo n les nombres du calcul un par un avant d'effectuer les opérations, plutôt que de tout calculer dans $\mathbb{Z}$ avant de réduire modulo n.

Exemples :

- La preuve par 9 est un test simple qui permet de contrôler la validité d'un calcul sur les entiers. Elle est enseignée au primaire car c'est un moyen rapide et élémentaire (mais pas infaillible) de vérifier que l'on a pas fait d'erreur dans ses multiplications « à la main ».

  La méthode consiste à exploiter le fait qu'un entier naturel est congru modulo 9 à la somme de ses chiffres pour reprendre le calcul initial, cette fois modulo 9. Si le nouveau calcul est vrai modulo 9, cela ne signifie pas à 100 % que le calcul de départ était juste mais la présomption est forte. Par contre, si le nouveau calcul n'est pas vrai modulo 9, on est certain qu'il y avait une erreur dans le calcul initial.

  Par exemple, un calcul à la main nous a donné $641 \times 6\,700\,417 = 4\,294\,967\,297$.

  Modulo 9, on a $641 \equiv 6 + 4 + 1 \equiv 2\ [9]$ et $6\,700\,417 \equiv 6 + 7 + 0 + 0 + 4 + 1 + 7 \equiv 7\ [9]$, donc $641 \times 6\,700\,417 \equiv 2 \times 7 \equiv 14 \equiv 5\ [9]$. Par ailleurs, on a $4\,294\,967\,297 \equiv 4 + 2 + \cdots + 7 \equiv 5\ [9]$. On peut donc bien penser que ce calcul est juste.

  En fait, 4 294 967 297 n'est pas n'importe quel entier. C'est le cinquième nombre de Fermat, c'est-à-dire $F_5 = 2^{2^5} + 1$.

  Fermat pensait que tous les nombres $F_n = 2^{2^n} + 1$, où $n \in \mathbb{N}$, étaient des nombres premiers ! Il se basait pour cela sur le fait que $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ et $F_4 = 65\,537$ sont effectivement premiers. Le calcul ci-dessus montre que F_5 n'est pas un nombre premier et infirme donc la conjecture de Fermat.

  Ce problème pourrait sembler anecdotique si Gauß n'avait pas montré que les nombres de Fermat premiers interviennent en géométrie : un polygone à n côtés est constructible à la règle et au compas si, et seulement si, n est le produit d'une puissance de 2 et de nombres de Fermat premiers distincts. En particulier, le polygone à 65 537 côtés est constructible !

  Aujourd'hui, on ne sait pas s'il existe des nombres de Fermat premiers autres que F_0, F_1, F_2, F_3 et F_4. On conjecture cependant que s'ils existent, ils sont rares !

D.2. L'anneau $\mathbb{Z}/n\mathbb{Z}$ [✠]

Dans tout ce paragraphe, n désigne un entier naturel non nul.

La compatibilité de la congruence modulo n avec l'addition et la multiplication permet de reconnaître une structure algébrique bien connue sur l'ensemble des classes de congruence.

Définition 11

Pour tout a dans $\mathbb{Z}$, on adopte la notation $\widehat{a}$ pour désigner la classe d'équivalence de a pour la relation $\equiv [n]$, c'est-à-dire $\widehat{a} = \{x \in \mathbb{Z} : x \equiv a\ [n]\}$. Cette classe est appelée la classe de congruence modulo n de l'entier a.

On rappelle que l'ensemble quotient est l'ensemble des classes d'équivalence modulo n. Il est noté $\mathbb{Z}/n\mathbb{Z}$ à la place de l'habituelle notation $\mathbb{Z}/\equiv$

La division euclidienne affirme que tout entier relatif a est congru modulo n à un entier r compris dans $[\![0; n-1]\!]$. Cet entier r est appelé le représentant principal de la classe de congruence de a modulo n.

L'ensemble quotient de $\mathbb{Z}$ pour la relation d'équivalence $\equiv [n]$ est donné par

$$\mathbb{Z}/n\mathbb{Z} = \left\{\widehat{0}; \widehat{1}; \ldots; \widehat{n-1}\right\},$$

où les classes $\widehat{0}; \widehat{1}; \ldots; \widehat{n-1}$ sont deux à deux disjointes.

■ La division euclidienne affirme que toute classe admet un représentant principal (c'est-à-dire dans $[\![0; n-1]\!]$), donc $\mathbb{Z}/n\mathbb{Z} = \left\{\widehat{0}; \widehat{1}; \ldots; \widehat{n-1}\right\}$.

Par ailleurs, deux entiers de $[\![0; n-1]\!]$ ne peuvent pas être congrus modulo n (l'écart entre les deux étant strictement inférieur à n), donc les classes $\widehat{0}; \widehat{1}; \ldots; \widehat{n-1}$ sont bien deux à deux disjointes. ■

On notera que $\widehat{0}$ est la classe des nombres entiers divisibles par n.

La compatibilité de la congruence avec $+$ et $\times$ implique le résultat suivant concernant $\mathbb{Z}/n\mathbb{Z}$.

Proposition 28

$\left(\mathbb{Z}/n\mathbb{Z}, +, \times\right)$ est un anneau commutatif.

■ Découle de vérifications techniques et de la proposition 27. ■

Dans la pratique, quand on calcule dans $\mathbb{Z}/n\mathbb{Z}$, on omet les petits chapeaux sur les classes. On confond donc constamment les classes et les représentants de celles-ci.

On notera en particulier que cette confusion est sans conséquence sur la relation « être premier avec n ». En effet, si un entier r est premier avec n, alors pour tout $k \in \mathbb{Z}$, le nombre $r + kn$ est également premier avec n (y réfléchir !), autrement dit tous les éléments de la classe de r sont premiers avec n. On peut donc dire, sans danger, que r est premier avec n sans avoir à préciser si r désigne un entier ou la classe modulo n de cet entier.

Exemples :

- Que vaut 2^{1975} dans $\mathbb{Z}/17\mathbb{Z}$?

  Vous pouvez essayez de faire la division euclidienne de 2^{1975} par 17 mais je vous préviens tout de suite, le quotient a 594 chiffres !

  Sinon, on constate que $2^4 \equiv -1\ [17]$ ou, si vous préférez, $2^4 = -1$ dans $\mathbb{Z}/17\mathbb{Z}$. Or $1975 = 493 \times 4 + 3$, donc, dans $\mathbb{Z}/17\mathbb{Z}$, on a

  $$2^{1975} = (2^4)^{493} \times 2^3 = (-1)^{493} \times 8 = -8 = 9.$$

La proposition suivante précise le groupe des inversibles de $\mathbb{Z}/n\mathbb{Z}$.

Proposition 29

On a

$$\mathrm{U}(\mathbb{Z}/n\mathbb{Z}) = \{r \in \mathbb{Z}/n\mathbb{Z} : r \wedge n = 1\}.$$

Le cardinal de $\mathrm{U}(\mathbb{Z}/n\mathbb{Z})$, c'est-à-dire le nombre d'entiers naturels non nuls inférieurs ou égaux à n qui sont premiers avec n, est noté $\varphi(n)$ et s'appelle l'indicatrice d'Euler de n.

■ On a

$$\begin{aligned} r \in \mathrm{U}(\mathbb{Z}/n\mathbb{Z}) &\iff \exists u \in \mathbb{Z}/n\mathbb{Z},\ ur = 1 \\ &\iff \exists u \in \mathbb{Z},\ ur \equiv 1\ [n] \\ &\iff \exists u, v \in \mathbb{Z},\ ur + vn = 1 \\ &\iff r \wedge n = 1, \end{aligned}$$

où la dernière équivalence découle du théorème de Bézout. ■

Cette démonstration en dit un peu plus sur les éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$. Pour déterminer l'inverse d'un élément r inversible (i.e. $r \wedge n = 1$), on recherche des coefficients de Bézout de r et n, c'est-à-dire deux entiers u et v tels que $ur + vn = 1$. L'inverse de r est alors u.

Exemples :

- Quel est l'inverse, s'il existe, de 7 dans $\mathbb{Z}/17\mathbb{Z}$? L'algorithme d'Euclide donne

q_i	r_i	u_i	v_i
	17	1	0
2	7	0	1
2	3	1	−2
3	1	−2	5
	0		

  donc $7 \wedge 17 = 1$ ce qui prouve que 7 est bien inversible dans $\mathbb{Z}/17\mathbb{Z}$. Par ailleurs, on a $-2 \times 17 + 5 \times 7 = 1$, ce qui donne $5 \times 7 \equiv 1\ [17]$ donc 5 est l'inverse de 7 dans $\mathbb{Z}/17\mathbb{Z}$.

Dans l'énoncé suivant, on envisage le cas où n est un nombre premier.

Proposition 30

L'anneau $(\mathbb{Z}/p\mathbb{Z}, +, \times)$ est un corps si, et seulement si, p est un nombre premier. Ce corps est noté $\mathbb{F}_p$. C'est un corps commutatif à p éléments.

■ On sait que p est premier si, et seulement si, p est premier avec tous les entiers naturels de $[\![1; p-1]\!]$, c'est-à-dire si, et seulement si, $\mathrm{U}(\mathbb{Z}/p\mathbb{Z}) = (\mathbb{Z}/p\mathbb{Z})^*$ ou encore si, et seulement si, $\mathbb{Z}/p\mathbb{Z}$ est un corps. ■

Il découle immédiatement de ce résultat que, lorsque p est premier, on a $\varphi(p) = p - 1$.

Exemples :

- Les éléments x de $\mathbb{F}_p$ qui sont leur propre inverse vérifie $x^2 = 1$, c'est-à-dire $x^2 - 1 = 0$ ou encore $(x-1)(x+1) = 0$, ce qui donne $x = \pm 1$ par intégrité (tout corps est intègre !).

  Dès lors, lorsqu'on calcule le produit de tous les éléments de $\mathbb{F}_p^*$, ils se simplifient tous par paire d'inversibles, sauf 1 et -1. Du coup, ce produit vaut -1. Comme ce produit vaut également $(p-1)!$, on en déduit que $(p-1)! = -1$ dans $\mathbb{F}_p$. Donc $(p-1)! \equiv -1\ [p]$.

  Réciproquement, si $(p-1)! \equiv -1\ [p]$, alors p est premier avec tous les entiers de $[\![1; p-1]\!]$ (car $(p-1)! \equiv -1\ [p]$ est une relation de Bézout). On en déduit que p est premier.

  On obtient ainsi le théorème de Wilson : p est premier si, et seulement si, $(p-1)! \equiv -1\ [p]$.

D.3. Petit théorème de Fermat

Commençons par un petit lemme de mise en bouche, où se mêle arithmétique et combinatoire.

Lemme 3

Soit p un nombre premier. Dans la ligne numérotée p du triangle de Pascal, tous les coefficients binomiaux, à l'exception du premier et du dernier (qui valent 1), sont divisibles par p. Autrement dit,

$$\forall k \in [\![1; p-1]\!], \qquad p \,\Big|\, \binom{p}{k}.$$

■ Soit $k \in [\![1; p-1]\!]$. La formule du pion nous dit que $k\binom{p}{k} = p\binom{p-1}{k-1}$, donc p divise $k\binom{p}{k}$. Or p est premier avec k (puisqu'un nombre premier est toujours premier avec les entiers non nuls qui le précèdent) donc, d'après le lemme de Gauß, p divise $\binom{p}{k}$. ■

On peut alors énoncer le petit théorème de Fermat.

Théorème 7

Soit p un nombre premier. Pour tout $a \in \mathbb{Z}$, on a

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

En particulier, pour tout entier a qui est premier avec p (c'est-à-dire a non divisible par p ou encore $a \not\equiv 0 \ [p]$), on a

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

■ ▶ La démonstration au programme !

▷ Démontrons tout d'abord que $\forall a \in \mathbb{Z},\ a^p \equiv a \ [p]$.

Notons d'abord que l'on a toujours $(-1)^p \equiv -1 \ [p]$. C'est vrai lorsque p est impair (puisque c'est alors une égalité « sans modulo ») et c'est aussi vraie pour $p = 2$ puisque $(-1)^2 \equiv 1 \equiv -1 \ [2]$.

Nous allons démontrer la propriété $\mathscr{P}(a)$: $a^p \equiv a \ [p]$ par une récurrence bidirectionnelle :-)

Initialisation : $\mathscr{P}(0)$ est vraie, je n'en dirai pas plus !

Hérédité : Fixons $a \in \mathbb{Z}$ tel que $\mathscr{P}(a)$ est vraie et démontrons $\mathscr{P}(a+1)$ et $\mathscr{P}(a-1)$. C'est en cela que la récurrence est bidirectionnelle ! Dans le calcul qui suit, toutes les occurences du symbole $\pm$ désignant un signe identique (parmi $+$ ou $-$), on a

$$(a \pm 1)^p = \sum_{k=0}^{p} \binom{p}{k} a^k (\pm 1)^{p-k} = \underbrace{a^p}_{\substack{\equiv\, a\ [p] \\ \text{par H.R.}}} + \underbrace{\sum_{k=1}^{p-1} \binom{p}{k} a^k (\pm 1)^{p-k}}_{\substack{\equiv\, 0\ [p] \\ \text{d'après le lemme 3}}} + \underbrace{(\pm 1)^p}_{\equiv\, \pm 1\ [p]} = a \pm 1 \ \ [p],$$

donc $\mathscr{P}(a+1)$ et $\mathscr{P}(a-1)$ sont vraies.

Conclusion : Par récurrence, $\mathscr{P}(a)$ est vraie pour tout $a \in \mathbb{Z}$, c'est-à-dire $\forall a \in \mathbb{Z},\ a^p \equiv a \ [p]$.

▷ Soit $a \in \mathbb{Z}$. Démontrons que si $a \wedge p = 1$, alors $a^{p-1} \equiv 1 \ [p]$.

Le cas précédent nous dit que $a^p \equiv a \ [p]$, c'est-à-dire $p \mid a^p - a$ ou encore $p \mid a(a^{p-1} - 1)$. Comme $a \wedge p = 1$, le lemme de Gauß implique alors que $p \mid a^{p-1} - 1$, c'est-à-dire $a^{p-1} \equiv 1 \ [p]$.

▶ Une démonstration utilisant $\mathbb{F}_p$.

▷ Cette fois, on démontre d'abord que si $a \wedge p = 1$, alors $a^{p-1} \equiv 1 \ [p]$, i.e. $\forall a \in \mathbb{F}_p^*,\ a^{p-1} = 1$.

Soit $a \in \mathbb{F}_p^*$. L'application $\sigma : \mathbb{F}_p^* \longrightarrow \mathbb{F}_p^*$ telle que $\forall x \in \mathbb{F}_p^*,\ \sigma(x) = xa$ est une bijection (de réciproque $x \longmapsto xa^{-1}$). C'est donc une permutation de $\mathbb{F}_p^*$. Dès lors, $\mathbb{F}_p^* = \{1, 2, \ldots, p-1\}$ peut encore s'écrire $\mathbb{F}_p^* = \{\sigma(1), \sigma(2), \ldots, \sigma(p-1)\} = \{a, 2a, \ldots, (p-1)a\}$. Du coup, le produit des éléments de $\mathbb{F}_p^*$ vaut à la fois $1 \times 2 \times \cdots \times (p-1)$ et $(a) \times (2a) \times \cdots \times \big((p-1)a\big)$, ce qui donne $(p-1)! = a^{p-1}(p-1)!$ Comme $(p-1)!$ est inversible (en tant que produit d'inversibles), on obtient $a^{p-1} = 1$.

▷ En multipliant cette relation par a, on obtient $a^p = a$ pour $a \in \mathbb{F}_p^*$. Reste à constater qu'elle est encore valable pour $a = 0$ pour conclure que $\forall a \in \mathbb{F}_p,\ a^p = a$, c'est-à-dire $\forall a \in \mathbb{Z},\ a^p \equiv a \ [p]$. ■

Exemples :

- Les nombres premiers impairs (c'est-à-dire tous les nombres premiers sauf 2) peuvent être rangés en deux catégories modulo 4 : ceux de la forme $1+4k$ avec $k \in \mathbb{N}^*$ et ceux de la forme $3+4k$ avec $k \in \mathbb{N}$.

  Considérons un nombre premier impair p pour lequel -1 est un carré modulo p. Nous allons démontrer que p est nécessairement de la forme $1+4k$ avec $k \in \mathbb{N}^*$.

  Pour cela, raisonnons par l'absurde en supposant qu'il existe $k \in \mathbb{N}$ tel que $p = 3+4k$, avec bien sûr l'hypothèse que -1 est un carré modulo ce nombre premier p. Il existe donc $a \in \mathbb{Z}$ tel que $-1 \equiv a^2\ [p]$. Nécessairement $a \not\equiv 0\ [p]$ sinon on aurait $-1 \equiv 0\ [p]$, ce qui est absurde. Le petit théorème de Fermat implique donc que

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

  Or

  $$a^{p-1} = a^{2+4k} = (a^2)^{1+2k} \equiv (-1)^{1+2k} \equiv -1\ \ [p]$$

  donc

  $$1 \equiv -1\ \ [p],$$

  c'est-à-dire

  $$p = 2,$$

  ce qui est absurde !

  On en conclut bien que p est de la forme $1+4k$ avec $k \in \mathbb{N}^*$.

8 h 00