Arithmétique

I. Divisibilité dans $\mathbb{Z}$

Diviseurs, multiples

1 **Définition.** Soit $a, b \in \mathbb{Z}$.

— On dit que b *divise* a, et l'on note $b \mid a$, lorsqu'il existe $k \in \mathbb{Z}$ tel que $a = kb$.

— On dit aussi que b est un *diviseur* de a, ou que a est un *multiple* de b.

— L'ensemble des diviseurs de $a \in \mathbb{Z}$ est noté $\mathscr{D}(a)$.

— L'ensemble des multiples de $b \in \mathbb{Z}$ est noté $b\mathbb{Z}$, c'est l'ensemble $\{bq,\ q \in \mathbb{Z}\}$.

- **Constats**
  — Les entiers 1 et -1 divisent tous les entiers, mais ne sont divisibles que par 1 et -1.
  — Tout nombre est un multiple de 1 et de lui-même (car $n = n \times 1$).
  — Tout nombre est un diviseur de 0 (car $0 = n \times 0$).
  — On a les égalités : $\mathscr{D}(a) = \mathscr{D}(-a)$ et $a\mathbb{Z} = (-a)\mathbb{Z}$.

- **Remarque pour tout le chapitre.**
  Pour tout ce qui concerne la divisibilité, on peut se limiter à $\mathbb{N}$ puisqu'un entier a les mêmes diviseurs et les mêmes multiples que son opposé. Cependant, les mathématiciens préfèrent travailler avec $\mathbb{Z}$ (car $\mathbb{Z}$ a une structure de *groupe* — allez voir les MPSI —, ce qui n'est pas le cas de $\mathbb{N}$).

- **Divisibilité VERSUS ordre naturel $\leqslant$**
  La relation de divisibilité sur $\mathbb{N}^*$ est liée à l'ordre naturel de $\mathbb{N}^*$ par la relation :

$$\forall\, a, b \in \mathbb{N}^*, \qquad a \mid b \implies a \leqslant b.$$

  Ce résultat est faux dans $\mathbb{N}$ puisque, par exemple, $1 \mid 0$, mais ~~$1 \leqslant 0$~~ .

  Ce résultat est faux dans $\mathbb{Z}$ puisque, par exemple, $3 \mid -6$, mais ~~$3 \leqslant -6$~~ .

2 preuve **Proposition (diviseurs d'un entier).** Soit $a \in \mathbb{Z}$.

— Si $a \neq 0$, alors $\mathscr{D}(a)$ est *inclus* dans $[\![-|a|, |a|]\!]$.

— Si $a = 0$, alors $\mathscr{D}(0)$ est égal à $\mathbb{Z}$.

3 **Proposition (multiples d'un entier).** Soit $a \in \mathbb{Z}$.
L'ensemble $a\mathbb{Z}$ contient 0, est symétrique par rapport à 0, stable par addition.

- **Cardinal de …**

  — Les diviseurs d'un entier *non nul* sont en nombre *fini*.
  En revanche, les diviseurs de 0 sont en nombre *infini* puisque tous les entiers divisent 0.

  — Les multiples d'un entier *non nul* sont en nombre *infini*.
  En revanche, les multiples de 0 sont en nombre *fini* puisque seul 0 est multiple de 0.

4 **Proposition (inclusion diviseurs/multiples).** Soit $a, b \in \mathbb{Z}$.
On a $b \mid a \iff a\mathbb{Z} \subset b\mathbb{Z}$
On a $b \mid a \iff \mathscr{D}(b) \subset \mathscr{D}(a)$

5 **Proposition.** Soit $a, b, c, d, a', b', u, v \in \mathbb{Z}$.

— **Transitivité.** Si $a \mid b$ et $b \mid c$, alors $a \mid c$.

— **Égalité au signe près.** On a $\Big(a \mid b \text{ et } b \mid a\Big) \iff \Big(a = b \text{ ou } a = -b\Big)$

— **Combinaison $\mathbb{Z}$-linéaire.** Si $d \mid a$ et $d \mid b$, alors $d \mid au + bv$.

Si d divise a et b, alors d divise toute combinaison linéaire de a et b à coefficients entiers.

— **Produit.** Si $b \mid a$ et $b' \mid a'$, alors $bb' \mid aa'$.

— **Puissance $k \in \mathbb{N}$.** Si $b \mid a$, alors $b^k \mid a^k$.

Division euclidienne sur $\mathbb{Z}$

6 preuve

Théorème (division euclidienne).
Soit $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$ *non nul.*
Il existe un unique couple $(q, r) \in \mathbb{Z}^2$ tel que $\begin{cases} a = bq + r \\ 0 \leqslant r < b. \end{cases}$

— q est appelé *quotient de la division euclidienne* de a par b,
— r est appelé *reste de la division euclidienne* de a par b.

- **Retour à l'école primaire.**
Effectuons la division euclidienne de 7342 par 31.

Expliquons la procédure apprise à l'école primaire.

$$\begin{aligned} 73 &= 31\times 2 + 11 \\ 734 &= 31\times 20 + \underbrace{114}_{31\times 3+21} \\ &= 31\times 23 + 21 \\ 7342 &= 31\times 230 + \underbrace{212}_{31\times 6+26} \\ &= 31\times 236 + 26 \end{aligned}$$

- **Remarque importante : lorsqu'on travaille dans $\mathbb{N}$.**
Si $a \in \mathbb{N}$, alors le quotient est également dans $\mathbb{N}$.

Preuve. On a $r < b$, d'où $a - bq < b$. Ainsi, $a < b(q+1)$.
Comme $a \in \mathbb{N}$, on a $0 < b(q+1)$.
Or $b > 0$ (car $b \in \mathbb{N}^*$), d'où $q + 1 > 0$. Donc $q \in \mathbb{N}$.

- **Passage par les réels.** On a $\begin{cases} a = bq + r \\ 0 \leqslant r < b \end{cases}$ d'où $\begin{cases} \dfrac{a}{b} = q + \dfrac{r}{b} \\ 0 \leqslant \dfrac{r}{b} < 1 \end{cases}$. Ainsi, $\dfrac{a}{b} = \underbrace{q}_{\in\mathbb{Z}} + \underbrace{\gamma}_{\in[0,1[}$. D'où $q = \lfloor \frac{a}{b} \rfloor$.

7 preuve

Proposition. Soit $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$.
On a l'équivalence :

$$b \text{ divise } a \iff \text{le reste de la division euclidienne de } a \text{ par } b \text{ est nul}$$

- **Plus généralement.** Pour montrer que r est le reste de la division euclidienne de a par b, il est équivalent de montrer que $r \in [\![0, b[\![$ et $b \mid a - r$.

8 sol → 21

Question.
Soit $u \in \mathbb{C}^{\mathbb{N}}$ une suite périodique, c'est-à-dire telle qu'il existe $a \in \mathbb{N}^*$ tel que $\forall n \in \mathbb{N},\ u_{n+a} = u_n$.
On note $\mathscr{P}_u$ l'ensemble des périodes de u :

$$\mathscr{P}_u = \left\{ p \in \mathbb{N}^* \mid \forall n \in \mathbb{N}, u_{n+p} = u_n \right\}$$

Justifier que $p_0 = \min \mathscr{P}_u$ est bien défini, puis montrer que $\mathscr{P}_u = p_0\mathbb{N}^*$.

II. Définition du pgcd et du ppcm

pgcd

Soit $a, b \in \mathbb{Z}$. Considérons l'ensemble $\mathscr{D}(a) \cap \mathscr{D}(b)$ des diviseurs communs à a et b.

— si $a = 0$ **et** $b = 0$; alors $\mathscr{D}(a) \cap \mathscr{D}(b) = \mathscr{D}(0) \cap \mathscr{D}(0) = \mathbb{Z} \cap \mathbb{Z} = \mathbb{Z}$.

— sinon (a, b *non tous les deux nuls*) ; alors $\mathscr{D}(a) \cap \mathscr{D}(b)$ est une partie de $\mathbb{Z}$:

  — non vide (car contient 1)

  — majorée (par $|a|$ si $a \neq 0$; par $|b|$ si $b \neq 0$)

Ainsi, $\mathscr{D}(a) \cap \mathscr{D}(b)$ possède un plus grand élément $\geqslant 1$.

9 **Définition.** Soit $a, b \in \mathbb{Z}$. On définit le pgcd de a et b de la façon suivante.

— Si $a = 0$ **et** $b = 0$, alors le pgcd de a et b est 0.

— Sinon (a et b *non tous les deux nuls* : $a \neq 0$ **ou** $b \neq 0$),
le pgcd de a et b est le plus grand des diviseurs communs à a et b.

Le pgcd est noté $\operatorname{pgcd}(a, b)$ ou encore $a \wedge b$.

- **Positivité.** Le pgcd est toujours un entier *naturel*.
- **Exemple.** On a $\mathscr{D}(-12) = \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12\}$ et $\mathscr{D}(15) = \{\pm 1, \pm 3, \pm 5, \pm 15\}$. Donc $\operatorname{pgcd}(-12, 15) = 3$.
- **Exit le signe moins.** Pour $a, b \in \mathbb{Z}$, on a $\operatorname{pgcd}(a, b) = \operatorname{pgcd}\big(|a|, |b|\big)$.

  Montrons par exemple $\operatorname{pgcd}(a, b) = \operatorname{pgcd}(a, -b)$ où $a, b \in \mathbb{Z}$. Il n'y a rien à montrer si $b = 0$. Supposons désormais $b \neq 0$.
  Comme $\mathscr{D}(b) = \mathscr{D}(-b)$, on a $\mathscr{D}(a) \cap \mathscr{D}(b) = \mathscr{D}(a) \cap \mathscr{D}(-b)$.
  Donc le plus grand élément de l'intersection de gauche, qui vaut $\operatorname{pgcd}(a, b)$ est égal au plus grand élément de l'intersection de droite, qui vaut $\operatorname{pgcd}(a, -b)$.
  Ce qui s'écrit $\operatorname{pgcd}(a, b) = \operatorname{pgcd}(a, -b)$.

- **Petites formules immédiates.** Soit $a, b \in \mathbb{Z}$. On a :

$$\operatorname{pgcd}(a, 0) = |a| \qquad \operatorname{pgcd}(a, 1) = 1 \qquad \text{si } b \mid a, \quad \operatorname{pgcd}(a, b) = |b|$$

10 **Définition.** Soit $a, b \in \mathbb{Z}$.
On dit que a et b sont *premiers entre eux* lorsque $\operatorname{pgcd}(a, b) = 1$.

- **Dans la pratique.** Pour montrer $\operatorname{pgcd}(a, b) = 1$, il suffit de prendre d un diviseur commun à a et b, et de montrer que $d \leqslant 1$ (ou bien, de manière équivalente, $d \mid 1$).

11 **Question.** Soit $a, b \in \mathbb{Z}$. On pose $\delta = \operatorname{pgcd}(a, b)$.
Montrer qu'il existe $a', b' \in \mathbb{Z}$ premiers entre eux tels que $a = \delta a'$ et $b = \delta b'$.
sol → 22

- **Ordre naturel VERSUS divisibilité.** Par définition, on a :

  Soit $a, b \in \mathbb{Z}$ non tous les deux nuls et $\delta \in \mathbb{Z}$.

$$\begin{cases} \delta \in \mathscr{D}(a) \cap \mathscr{D}(b) \\ \forall\, d \in \mathscr{D}(a) \cap \mathscr{D}(b),\ d \leqslant \delta \end{cases} \iff \delta = \operatorname{pgcd}(a, b)$$

  Il existe le même genre de résultat en remplaçant « plus petit que $\leqslant$ » par « divise $\mid$ ».
  Pour l'instant, seule l'implication $\Longrightarrow$ est facile à justifier :

  Soit $a, b \in \mathbb{Z}$. Soit $\delta \in \mathbb{N}$.
  On a :

$$\begin{cases} \delta \in \mathscr{D}(a) \cap \mathscr{D}(b) \\ \forall\, d \in \mathscr{D}(a) \cap \mathscr{D}(b),\ d \mid \delta \end{cases} \Longrightarrow \delta = \operatorname{pgcd}(a, b)$$

  — Les deux conditions de gauche sont invariantes par $\delta \leftrightarrow -\delta$, d'où le besoin d'imposer $\delta \in \mathbb{N}$.

  — On remarque que cette caractérisation englobe le cas où a et b sont nuls tous les deux.
  En effet, dans ce cas, la deuxième condition s'écrit $\forall\, d \in \mathbb{Z},\ d \mid \delta$. En prenant $d = 0$, on obtient $\delta = 0$.

ppcm

Soit $a, b \in \mathbb{Z}$. Considérons l'ensemble $a\mathbb{Z} \cap b\mathbb{Z}$ des multiples communs à a et b.

— si $a = 0$ **ou** $b = 0$; alors $a\mathbb{Z} \cap b\mathbb{Z} = \{0\}$.

— sinon (a, b *tous les deux non nuls*) ; alors $a\mathbb{Z} \cap b\mathbb{Z}$ est une partie de $\mathbb{Z}$.
Son intersection avec $\mathbb{N}^*$ est une partie de $\mathbb{N}$ non vide (car contient $|a||b|$).
Ainsi, $a\mathbb{Z} \cap b\mathbb{Z} \cap \mathbb{N}^*$ possède un plus petit élément $\geqslant 1$.

12 **Définition.** Soit $a, b \in \mathbb{Z}$. On définit le ppcm de a et b de la façon suivante.

— Si $a = 0$ **ou** $b = 0$, alors le ppcm de a et b est 0.

— Sinon (a et b *tous les deux non nuls* : $a \neq 0$ **et** $b \neq 0$),
le ppcm de a et b est le plus petit des multiples *strictement positifs* communs à a et b.

Le ppcm est noté $\text{ppcm}(a, b)$ ou encore $a \vee b$.

- **Positivité.** Le ppcm est toujours un entier *naturel*.
- **Exemple.** On a $(-12)\mathbb{Z} \cap \mathbb{N}^* = \{12, 24, 36, 48, 60, 72, \ldots\}$ et $15\mathbb{Z} \cap \mathbb{N}^* = \{15, 30, 45, 60, 75, \ldots\}$.
Donc $\text{ppcm}(-12, 15) = 60$.
- **Exit le signe moins.** Pour $a, b \in \mathbb{Z}$, on a $\text{ppcm}(a, b) = \text{ppcm}\big(|a|, |b|\big)$.
- **Petites formules immédiates.** Soit $a, b \in \mathbb{Z}$. On a :

$$\text{ppcm}(a, 0) = 0 \qquad \text{ppcm}(a, 1) = |a| \qquad \text{si } b \mid a, \quad \text{ppcm}(a, b) = |a|$$

- **Utilité ?** Quand on fait la somme de deux fractions comme $\frac{3}{16} + \frac{5}{12}$, on les réduit au même dénominateur, c'est-à-dire qu'on les écrit comme des fractions dont le dénominateur est égal au ppcm des dénominateurs originaux. Comme $\text{ppcm}(16, 12) = 48$, on a

$$\frac{3}{16} + \frac{5}{12} = \frac{9}{48} + \frac{20}{48} = \frac{29}{48}$$

- **Ordre naturel VERSUS divisibilité.** Par définition, on a :

Soit $a, b \in \mathbb{Z}$ tous les deux non nuls et $\mu \in \mathbb{Z}$.

$$\begin{cases} \mu \in a\mathbb{Z} \cap b\mathbb{Z} \cap \mathbb{N}^* \\ \forall\, m \in a\mathbb{Z} \cap b\mathbb{Z} \cap \mathbb{N}^*,\ m \geqslant \mu \end{cases} \iff \mu = \text{ppcm}(a, b)$$

Il existe le même genre de résultat en remplaçant l'ordre naturel par la relation de divisibilité.
Pour l'instant, seule l'implication $\Longrightarrow$ est facile à justifier :

Soit $a, b \in \mathbb{Z}$. Soit $\mu \in \mathbb{N}$.
On a :

$$\begin{cases} \mu \in a\mathbb{Z} \cap b\mathbb{Z} \\ \forall\, m \in a\mathbb{Z} \cap b\mathbb{Z},\ m \in \mu\mathbb{Z} \end{cases} \Longrightarrow \mu = \text{ppcm}(a, b)$$

— Les deux conditions de gauche sont invariantes par $\mu \leftrightarrow -\mu$, d'où le besoin d'imposer $\mu \in \mathbb{N}$.

— On remarque que cette caractérisation englobe le cas où l'un des entiers a ou b est nul.
En effet, dans ce cas, la première condition s'écrit $\mu \in 0\mathbb{Z} \cap b\mathbb{Z}$ ou bien $\mu \in a\mathbb{Z} \cap 0\mathbb{Z}$. On obtient bien $\mu = 0$.

— On voit que l'énoncé est plus clair car il ne fait intervenir que « du $\mathbb{Z}$ » : il n'y a pas de vilaine intersection avec $\mathbb{N}^*$.

III. Algorithme d'Euclide

13 **Le lemme des informaticiens.**
Il n'existe pas de suite strictement décroissante d'entiers naturels.
Autrement dit, une suite strictement décroissante d'entiers naturels est toujours finie.

14 **Le lemme fondamental du cours d'arithmétique de PCSI.**
Soit $a, b, q, r \in \mathbb{Z}$ tels que $a = bq + r$.
Alors $\mathscr{D}(a) \cap \mathscr{D}(b) = \mathscr{D}(b) \cap \mathscr{D}(r)$.
En particulier, $\text{pgcd}(a, b) = \text{pgcd}(b, r)$.

- **Remarque.** Ici, l'égalité $a = bq + r$ n'est *pas* supposée être la division euclidienne de a par b.
- **Autre formulation amusante.**
  Si $a = bq + r$ (avec aucune condition sur b et r), alors $a \wedge b = b \wedge r$.
  Ce que l'on peut écrire $(bq + r) \wedge b = b \wedge r$, ou encore $b \wedge (r + bq) = b \wedge r$.
  Autrement dit, en lisant la formule de gauche à droite, on voit que l'on peut retirer un multiple du premier indice.
- **Algorithme d'Euclide**
  Avec ce lemme, on a un moyen pour calculer le pgcd de a et b.
  - Si $b = 0$, alors $\text{pgcd}(a, b) = |a|$.
  - Si $b \neq 0$, alors on écrit la division euclidienne de a par b, disons $a = bq + r$, puis on recommence en remplaçant (a, b) par (b, r).
    La suite des restes obtenue est strictement décroissante, et est une suite d'entiers naturels.
    D'après le lemme des informaticiens, la suite est *finie*.
    Le pgcd de a et b est alors le dernier reste non nul, **qui est aussi le dernier diviseur non nul**.
- **Exemple 1.** Soit $a = 19$ et $b = 7$. On a les divisions euclidiennes successives suivantes :

$$\begin{array}{rclcll} a & = & bq_1 & + & c & \text{avec } q_1 = 2 \text{ et } c = 5 \\ b & = & cq_2 & + & d & \text{avec } q_2 = 1 \text{ et } d = 2 \\ c & = & dq_3 & + & e & \text{avec } q_3 = 2 \text{ et } e = 1 \\ d & = & eq_4 & + & 0 & \text{avec } q_4 = 2 \end{array}$$

  On en déduit
$$a \wedge b = b \wedge c = c \wedge d = d \wedge e = e \wedge 0 = e$$
  Donc le pgcd de 19 et 7 est $e = 1$.
- **Exemple 2.** Soit $a = 782$ et $b = 221$. On a les divisions euclidiennes successives suivantes :

$$\begin{array}{rclcll} a & = & bq_1 & + & c & \text{avec } q_1 = 3 \text{ et } c = 119 \\ b & = & cq_2 & + & d & \text{avec } q_2 = 1 \text{ et } d = 102 \\ c & = & dq_3 & + & e & \text{avec } q_3 = 1 \text{ et } e = 17 \\ d & = & eq_4 & + & 0 & \text{avec } q_4 = 6 \end{array}$$

  On en déduit
$$a \wedge b = b \wedge c = c \wedge d = d \wedge e = e \wedge 0 = e$$
  Donc le pgcd de 782 et 221 est 17.
- **Remarque anecdotique.** Lorsque $a < b$, l'algorithme commence donc par échanger a et b (WHY ?).

IV. Nombres premiers

Premières propriétés

15 **Définition.** On appelle *nombre premier* tout entier naturel différent de 1 n'admettant pour diviseurs *positifs* que 1 et lui-même.

- **Exemple.** Les entiers 2, 3, 5, 7, 11, …, 65 537, …, 314 159, …, 2 718 281, … sont premiers.
- **Remarque importante pour les exos.** Un nombre premier p est $\geqslant 2$.
  Par conséquent, si au cours d'une *preuve par l'absurde*, on tombe sur $p \mid 1$, c'est gagné !
- **Reformulation** Soit p un nombre premier et $a, b \in \mathbb{Z}$ tels que $p = ab$. Alors $a = \pm 1$ ou $b = \pm 1$.
- **Négation.** Un entier $n \geqslant 2$ est non premier si et seulement s'il existe $d \in [\![2, n-1]\!]$ tel que $d \mid n$.

16 **Question.** Soit $a \geqslant 3$ et $n \geqslant 2$. Montrer que $a^n - 1$ n'est pas premier.

17 preuve **Proposition.**
— Tout entier $n \geqslant 2$ admet un diviseur premier.
— Si $n \geqslant 2$ n'est pas premier, il admet un diviseur premier inférieur ou égal à $\sqrt{n}$.

- **Application.** Pour savoir si un nombre $\leqslant 100$ est premier, il suffit de vérifier qu'il n'est ni multiple de 2, ni multiple de 3, ni multiple de 5, ni multiple de 7 (les seuls multiples de 7 à connaître au-delà de la table usuelle sont 77 et 91).
- **Le crible d'Ératosthène.**
  Il permet de déterminer tous les nombres premiers inférieurs ou égaux à un entier n fixé en constatant :
  — 2 est le premier nombre premier ; cela empêche tous les autres nombres pairs d'être premiers : on les raye.
  — Le premier nombre non rayé (à savoir 3) n'est donc pas divisible par 2 : il est donc premier. On peut alors rayer tous les multiples de 3.
  — Le premier nombre non rayé (à savoir 5) n'est donc pas divisible par les nombres premiers inférieur à lui : il est donc premier. On peut alors rayer tous les multiples de 5.
  — L'algorithme s'arrête quand on dépasse strictement $\sqrt{n}$.
  — Les nombres appartenant à $[\![2, n]\!]$ qui n'ont pas été rayés sont alors les nombres premiers $\leqslant n$.

	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

18 **Proposition.** L'ensemble des nombres premiers est infini.

- **Première preuve.** Montrons que $\mathscr{P}$ est infini en raisonnant par l'absurde.
  Supposons $\mathscr{P}$ fini. On peut donc considérer le produit suivant $\prod_{p\in\mathscr{P}} p$.
  Considérons l'entier $N = \left(\prod_{p\in\mathscr{P}} p\right) + 1$, qui est $\geqslant 2$.
  L'entier N admet un diviseur premier $q \in \mathscr{P}$ (WHY?).
  On a (WHY?) $q \mid 1$.
  C'est absurde (WHY?).
- **Deuxième preuve.** Montrons que l'ensemble des nombres premiers est non majoré.
  Soit $n \in \mathbb{N}$. Montrons qu'il existe un nombre premier $p > n$.
  Considérons l'entier $N = n! + 1$ qui est $\geqslant 2$.
  L'entier N admet un diviseur premier p.
  Montrons que $p > n$. Raisonnons par l'absurde.
  Si on avait $p \leqslant n$, alors p diviserait $n!$. Comme p divise N, alors p diviserait leur différence à savoir 1.
  Ce qui est impossible car p est premier.
  Donc $p > n$.

Décomposition en facteurs premiers

19 **Théorème admis (Décomposition en Facteurs Premiers = DFP).**
Tout entier $\geqslant 2$ s'écrit de manière unique, à l'ordre près des facteurs, comme un produit de nombres premiers.

- **Exemples.** On a

  $12 = \ldots$ $\qquad$ $144 = \ldots$ $\qquad$ $42 = \ldots$

- **En maths.** Soit $n \geqslant 2$.
  Il existe une unique partie $\{p_1, \ldots, p_r\}$ de $\mathscr{P}$, un unique r-uplet $(\alpha_1, \ldots, \alpha_r) \in \mathbb{N}^*$ d'exposants strictement positifs tels que :
  $$n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$$
  Les nombres premiers $p_1, \ldots, p_r$ sont appelés les *facteurs premiers* de n.
  On peut même donner un sens au théorème avec $n = 1$ en prenant la partie vide.
- **Avec exposants dans $\mathbb{N}$.**
  La condition « $\alpha_i \in \mathbb{N}^*$ » sert à donner un énoncé simple de l'*unicité* de la décomposition en facteurs premiers, mais il est souvent pratique d'autoriser une décomposition plus générale de la forme
  $$n = p_1^{\beta_1} \cdots p_s^{\beta_s} \quad \text{avec } \beta_i \in \mathbb{N}$$
  Autrement dit, on peut écrire 75 sous la forme $75 = 3 \times 5^2$, mais également sous la forme $75 = 2^0 \times 3 \times 5^2$.
  Cela est notamment utile si l'on veut décomposer deux entiers et comparer leur DFP.
  Par exemple, $75 = 2^0 \times 3 \times 5^2$ et $5 = 2^0 \times 3^0 \times 5$.

Le théorème précédent est admis (programme officiel), mais je vous propose deux preuves de l'existence de la DFP. L'unicité est pour l'instant hors de portée.

- **Par récurrence forte.**

  Pour tout $n \geqslant 2$, notons $\mathscr{H}_n$ la propriété « n est un produit de nombres premiers ».

  Initialisation. 2 est un nombre premier, donc est un produit de nombres premiers.

  Donc $\mathscr{H}_2$ est vraie.

  Hérédité. Soit $n \geqslant 2$.

  On suppose $\mathscr{H}_2, \mathscr{H}_3, \ldots, \mathscr{H}_n$.

  Montrons $\mathscr{H}_{n+1}$.

  Distinguons deux cas.

  — Si $n+1$ est premier, il est en particulier un produit de nombres premiers.

  — Si $n+1$ n'est pas premier, on peut trouver deux entiers a et b, appartenant à $[\![2, n]\!]$, tels que $n+1 = ab$.

  D'après l'hypothèse de récurrence, $\mathscr{H}_a$ et $\mathscr{H}_b$ sont vraies.

  Donc a et b sont produits de nombres premiers.

  On peut donc trouver des nombres premiers $p_1, \ldots, p_r$ et $q_1, \ldots, q_s$ (pas nécessairement distincts) tels que

  $$a = p_1 \cdots p_r \qquad \text{et} \qquad b = q_1 \cdots q_s$$

  En effectuant le produit, on a alors $ab = p_1 \cdots p_r q_1 \cdots q_s$.

  Ainsi $n+1$ est un produit de nombres premiers.

  Dans les deux cas, $n+1$ est un produit de nombres premiers, ce qui démontre $\mathscr{H}_{n+1}$.

- **Par absurde-minimalité.**

  Raisonnons par l'absurde et supposons qu'il existe des entiers $\geqslant 2$ qui ne soit **pas** produit de nombres premiers. Notons E l'ensemble de ces nombres.

  Alors E est une partie de $\mathbb{N}$ non vide (WHY ?).

  Donc E admet un plus petit élément. Posons $m = \min E$.

  Alors m n'est pas premier (WHY ?).

  Donc il existe $a, b \in [\![2, m-1]\!]$ tels que $m = ab$.

  Par minimalité de m, les entiers a et b ne sont pas dans E (WHY ?).

  Donc a et b sont des produits de nombres premiers.

  Mais alors leur produit, à savoir m, est également un produit de nombres premiers.

  D'où la contradiction.

Conséquences de la DFP

20 preuve

Proposition (diviseurs avec DFP).
Soit $n \in \mathbb{N}^*$ dont la décomposition en facteurs premiers est $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$.
Alors, les diviseurs positifs de n sont les entiers d qui s'écrivent :

$$d = p_1^{\delta_1} \cdots p_r^{\delta_r} \quad \text{où } \forall\, i \in [\![1, r]\!],\ 0 \leqslant \delta_i \leqslant \alpha_i$$

- **Corollaire (critère de divisibilité avec DFP).**
  Soit $a, b \in \mathbb{N}^*$ que l'on écrit $a = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ et $b = p_1^{\beta_1} \cdots p_r^{\beta_r}$ où $p_1, \ldots, p_r$ sont des nombres premiers distincts et $\alpha_i, \beta_i \in \mathbb{N}$.
  On a l'équivalence :

$$a \mid b \iff \forall\, i \in [\![1, r]\!],\ \alpha_i \leqslant \beta_i$$

21 **Question.** Soit $a, b \in \mathbb{N}^*$ tel que $a^2 \mid b^2$. Montrer que $a \mid b$.

22 preuve

Proposition (pgcd et ppcm).
Soit $a, b \in \mathbb{N}^*$ que l'on écrit

$$a = p_1^{\alpha_1} \cdots p_r^{\alpha_r} \quad \text{et} \quad b = p_1^{\beta_1} \cdots p_r^{\beta_r},$$

où $p_1, \ldots, p_r$ sont des nombres premiers distincts et $\alpha_i, \beta_i \in \mathbb{N}$.
Alors on a :

$$\operatorname{pgcd}(a, b) = \prod_{i=1}^{r} p_i^{\min(\alpha_i, \beta_i)} \quad \text{et} \quad \operatorname{ppcm}(a, b) = \prod_{i=1}^{r} p_i^{\max(\alpha_i, \beta_i)}.$$

- **Pour déterminer le pgcd**, nous disposons donc ou bien de l'algorithme d'Euclide, ou bien de la décomposition en facteurs premiers.
- **Exemple.** Calculons le pgcd de $a = 201387$ et $b = 3000$.
  La décomposition en facteurs premiers de b est immédiate $3000 = 2^3 \times 3 \times 5^3$.
  Le pgcd recherché est donc de la forme $2^\alpha \times 3^\beta \times 5^\gamma$, avec $\alpha \leqslant 3$, puis $\beta \leqslant 1$ et $\gamma \leqslant 3$.
  La décomposition en facteurs premiers de a est « ce qu'elle est », mais une chose est sûre, elle ne fait pas apparaître 2 et 5, et contient un terme du type 3^x avec $x \geqslant 1$ (en effet, a est divisible par 3, WHY ?).
  On en déduit que $\operatorname{pgcd}(a, b) = 3^{\min(1, x)}$, donc $\operatorname{pgcd}(a, b) = 3$.

23 preuve

Proposition (produit pgcd-ppcm, avec DFP). Soit $a, b \in \mathbb{Z}$. On a l'égalité

$$\operatorname{pgcd}(a, b) \times \operatorname{ppcm}(a, b) = |a||b|$$

En particulier, le ppcm de deux entiers naturels premiers entre eux est égal à leur produit.

V. Caractérisation du pgcd et du ppcm (HP)

24 preuve

Proposition. Soit $a, b \in \mathbb{Z}$.
On a $\mathscr{D}(a) \cap \mathscr{D}(b) = \mathscr{D}(a \wedge b)$.

- **Idée de la preuve.** Commencer par $b \in \mathbb{N}$ et noter $\mathscr{H}_b$: « Pour tout $a \in \mathbb{Z}$, on a $\mathscr{D}(a) \cap \mathscr{D}(b) = \mathscr{D}(a \wedge b)$ ».
- **Explication.** L'inclusion $\mathscr{D}(a) \cap \mathscr{D}(b) \subset \mathscr{D}(a \wedge b)$ n'est pas du tout évidente (l'autre est gratuite ou presque).
  Elle s'énonce :

  Tout diviseur de a et b est un diviseur de leur pgcd.

  Autrement dit, $\text{pgcd}(a, b)$ est le plus grand élément de $\mathscr{D}(a) \cap \mathscr{D}(b)$ *pour la relation de divisibilité* sur $\mathbb{N}$.
- **Reformulation avec une équivalence.** L'égalité précédente s'écrit :

  Soit $\delta \in \mathbb{N}$. On a :

$$\begin{cases} \delta \in \mathscr{D}(a) \cap \mathscr{D}(b) \\ \forall\, d \in \mathscr{D}(a) \cap \mathscr{D}(b),\ d \mid \delta \end{cases} \iff \delta = \text{pgcd}(a, b)$$

  ou encore

$$\begin{cases} \delta \in \mathscr{D}(a) \cap \mathscr{D}(b) \\ \mathscr{D}(a) \cap \mathscr{D}(b) \subset \mathscr{D}(\delta) \end{cases} \iff \delta = \text{pgcd}(a, b)$$

  ou encore

$$\mathscr{D}(a) \cap \mathscr{D}(b) = \mathscr{D}(\delta) \iff \delta = \text{pgcd}(a, b)$$

  Ainsi, cette équivalence montre que le pgcd est le seul entier naturel δ à vérifier $\mathscr{D}(a) \cap \mathscr{D}(b) = \mathscr{D}(\delta)$.

25 preuve

Proposition. Soit $a, b \in \mathbb{Z}$.
On a $a\mathbb{Z} \cap b\mathbb{Z} = (a \vee b)\mathbb{Z}$.

- **Idée de la preuve.** Pour $m \in a\mathbb{Z} \cap b\mathbb{Z}$, écrire la division euclidienne de m par μ.
- **Explication.** L'inclusion $a\mathbb{Z} \cap b\mathbb{Z} \subset (a \vee b)\mathbb{Z}$ n'est pas du tout évidente (l'autre est gratuite ou presque).
  Elle s'énonce :

  Tout multiple de a et b est un multiple de leur ppcm.

  Autrement dit, $\text{ppcm}(a, b)$ est le plus petit élément de $a\mathbb{Z} \cap b\mathbb{Z}$ *pour la relation de divisibilité* sur $\mathbb{N}$.
- **Reformulation avec une équivalence.** L'égalité précédente s'écrit :

  Soit $\mu \in \mathbb{N}$. On a :

$$\begin{cases} \mu \in a\mathbb{Z} \cap b\mathbb{Z} \\ \forall\, m \in a\mathbb{Z} \cap b\mathbb{Z},\ m \in \mu\mathbb{Z} \end{cases} \iff \mu = \text{ppcm}(a, b)$$

  ou encore

$$\begin{cases} \mu \in a\mathbb{Z} \cap b\mathbb{Z} \\ a\mathbb{Z} \cap b\mathbb{Z} \subset \mu\mathbb{Z} \end{cases} \iff \mu = \text{ppcm}(a, b)$$

  ou encore

$$a\mathbb{Z} \cap b\mathbb{Z} = \mu\mathbb{Z} \iff \mu = \text{ppcm}(a, b)$$

  Ainsi, cette équivalence montre que le ppcm est le seul entier naturel μ à vérifier $a\mathbb{Z} \cap b\mathbb{Z} = \mu\mathbb{Z}$.

VI. Conséquences multiples ! (HP)

Homogénéité du pgcd et du ppcm

26 preuve

Proposition (homogénéité). Soit $a, b \in \mathbb{Z}$. Soit $k \in \mathbb{N}$. Alors

$$\text{pgcd}(ka, kb) = k\,\text{pgcd}(a, b)$$

- **Corollaire.** On en déduit facilement (WHY ?) :
  Soit $a, b, a', b' \in \mathbb{Z}$ et $d \in \mathbb{N}$ tels que $a = da'$ et $b = db'$.
  Si $\text{pgcd}(a', b') = 1$, alors $d = \text{pgcd}(a, b)$.
- **Idem.** On a le même type d'énoncé avec le ppcm.

Le lemme de Gauss et ses corollaires

27 preuve

Lemme de Gauss. Soit $a, b, c \in \mathbb{Z}$.

$$\begin{cases} a \mid bc \\ a \wedge b = 1 \end{cases} \implies a \mid c$$

28

Lemme d'Euclide. Soit $a, b \in \mathbb{Z}$ et $p \in \mathscr{P}$.

$$p \mid ab \implies \Big(p \mid a \quad \text{ou} \quad p \mid b \Big)$$

- **Remarque.**
  Le lemme d'Euclide est en fait un corollaire du lemme de Gauss, car il est équivalent à (WHY ?)

$$\begin{cases} p \mid ab \\ p \wedge a = 1 \end{cases} \implies p \mid b$$

- **Remarque.** Pour un nombre premier $p \in \mathscr{P}$, on a $p \nmid a \implies p \wedge a = 1$.
  Attention, cela nécessite que p soit un nombre premier. On a $4 \nmid 6$ mais ~~$4 \wedge 6 = 1$~~ .
- On a la généralisation suivante.
  Lemme d'Euclide généralisé. *Soit $a_1, \dots, a_r \in \mathbb{Z}$ et $p \in \mathscr{P}$.*
  Si $p \mid a_1 \cdots a_r$, alors il existe $i \in [\![1, r]\!]$ tel que $p \mid a_i$.
- Et encore une généralisation :
  Lemme d'Euclide avec puissance. *Soit $b_1, \dots, b_r \in \mathbb{Z}$, $\beta_1, \dots, \beta_r$ et $p \in \mathscr{P}$.*
  Si $p \mid b_1^{\beta_1} \cdots b_r^{\beta_1}$, alors il existe $i \in [\![1, r]\!]$ tel que $p \mid b_i$.

Proposition (produit pgcd-ppcm, sans DFP, avec Gauss). Soit a et $b \in \mathbb{Z}$.

— Si a et b sont premiers entre eux, alors $a \vee b = |a||b|$.
Cela signifie :

$$a \wedge b = 1 \implies a\mathbb{Z} \cap b\mathbb{Z} = |a||b|\mathbb{Z} \qquad \text{ou encore, car l'inclusion } \supset \text{ est auto} \qquad \forall m \in \mathbb{Z},\ \begin{cases} a \mid m \\ b \mid m \\ a \wedge b = 1 \end{cases} \implies ab \mid m.$$

— Plus généralement, on a $(a \vee b)(a \wedge b) = |a||b|$.

Preuve. Soit $m \in \mathbb{Z}$ tel que $a \mid m$ et $b \mid m$.
Alors il existe $k \in \mathbb{Z}$ tel que $m = ak$.
Donc $b \mid ak$. Comme $a \wedge b = 1$, on en déduit que $b \mid k$, d'après le lemme de Gauss.
Donc $k = bk'$.
D'où $m = abk'$. D'où $ab \mid m$.

On écrit $a = da'$ et $b = db'$ avec des bonnes notations !
D'après le point précédent, on a $a' \vee b' = |a'||b'|$.
En multipliant par d^2, et en exploitant l'homogénéité du ppcm, on a $d \times (a \vee b) = |a||b|$. C'est-à-dire $(a \wedge b)(a \vee b) = |a||b|$.

Démonstration de l'unicité de la DFP

Soit $n \geqslant 2$ que l'on écrit de deux façons

$$n = p_1^{\alpha_1} \cdots p_r^{\alpha_r} \qquad \text{et} \qquad n = q_1^{\beta_1} \cdots q_s^{\beta_s}$$

où les $p_i \in \mathscr{P}$ sont deux à deux distincts et $\alpha_i \in \mathbb{N}^*$ (idem pour les q_j et β_j).

— Montrons d'abord $\{p_1, \ldots, p_r\} \subset \{q_1, \ldots, q_s\}$.
Soit $i \in [\![1, r]\!]$.
On a $p_i \mid n$, donc $p_i \mid q_1^{\beta_1} \cdots q_s^{\beta_s}$.
Comme $p_i \in \mathscr{P}$, le résultat précédent (lequel ?) implique qu'il existe $k \in [\![1, s]\!]$ tel que $p_i \mid q_k$.
Comme $q_k \in \mathscr{P}$, on a nécessairement $p_i = 1$ ou $p_i = q_k$.
Mais $p_i \neq 1$, donc $p_i = q_k$.
Donc $p_i \in \{q_1, \ldots, q_s\}$.

— Par symétrie des données, on obtient $\{p_1, \ldots, p_r\} \supset \{q_1, \ldots, q_s\}$.

— On en déduit que $r = s$. Puis, quitte à réordonner, on obtient $\forall\, i,\ p_i = q_i$.

— Montrons que $\forall\, i,\ \alpha_i = \beta_i$.
Supposons par l'absurde qu'il existe i_0 tel que $\alpha_{i_0} \neq \beta_{i_0}$.
Quitte à échanger les rôles, on peut supposer que $\alpha_{i_0} > \beta_{i_0}$.
On a

$$\left(\prod_{k \neq i_0} p_k^{\alpha_k}\right) \times p_{i_0}^{\alpha_{i_0} - \beta_{i_0}} = \left(\prod_{k \neq i_0} p_k^{\beta_k}\right)$$

Comme $\alpha_{i_0} - \beta_{i_0} \geqslant 1$, on a $p_{i_0} \mid \left(\prod_{k \neq i_0} p_k^{\beta_k}\right)$.
Comme p_{i_0} est premier, p_{i_0} divise un terme du produit d'après le lemme d'Euclide généralisé : ainsi, il existe $k \neq i_0$ tel que $p_{i_0} \mid p_k$, ce qui est impossible, car p_k est premier.

VII. Bézout and Cie (HP)

Le théorème de Bézout

29 **Question.** Trouver tous les couples $(u,v) \in \mathbb{Z}^2$ tels que $3u+5v=2024$.

30 preuve

Théorème de Bézout. Soit $a,b \in \mathbb{Z}$.
Il existe $u,v \in \mathbb{Z}$ tels que $au+bv = \text{pgcd}(a,b)$.

- **Preuve.** Elle peut se faire par récurrence forte, en commençant par le cas $b \in \mathbb{N}$ et en considérant $\mathscr{H}_b$ la propriété « Pour tout $a \in \mathbb{Z}$, il existe $u,v \in \mathbb{Z}$ tel que $au+bv = \text{pgcd}(a,b)$ ».
- **Remarque.** Il n'y a pas d'unicité du couple (u,v).
  Pire, avec un couple solution, on en crée une infinité.
  En effet, si (u,v) est un couple de Bézout, alors $(u-mb, v+ma)$ en est un aussi pour tout $m \in \mathbb{Z}$, car $au+bv = a(u-mb)+b(v+ma)$.
- **Attention.** Si on a $au+bv=d$, alors cela n'implique pas que d est égal au $\text{pgcd}(a,b)$.
  Par exemple, il existe $u,v \in \mathbb{Z}$ tels que $3u+5v=2024$ et pourtant 2024 n'est pas égal à $\text{pgcd}(3,5)=1$.
  En revanche, si on a une relation du type $au+bv=d$, alors $\text{pgcd}(a,b) \mid d$ (WHY ?).

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

Obtention du pgcd et des coefficients de Bézout

Soit $a,b \in \mathbb{Z}$ avec $b \neq 0$.
Supposons que les divisions euclidiennes successives soient les suivantes :

$$\begin{array}{rcl} a &=& bq_1 + c \\ b &=& cq_2 + d \\ c &=& dq_3 + e \\ d &=& eq_4 + 0 \end{array}$$

Le pgcd de a et b est donc e.
Comment obtenir **des** coefficients de Bézout, c'est-à-dire $u,v \in \mathbb{Z}$ tels que $au+bv=e$?
L'idée est la suivante. On part de l'avant-dernière égalité dont le reste est le pgcd e, puis on remonte.

$$\begin{array}{rcll} e &=& c - dq_3 & 3^{\text{ème}} \text{ égalité pour exprimer } e \\ &=& c-(b-cq_2)q_3 & 2^{\text{ème}} \text{ égalité pour exprimer } d \\ &=& b(-q_3)+c(1+q_2q_3) & \text{calculs : on isole } b \text{ et } c \\ &=& b(-q_3)+(a-bq_1)(1+q_2q_3) & 1^{\text{ère}} \text{ égalité pour exprimer } c \\ &=& a(1+q_2q_3)+b\big(-q_1(1+q_2q_3)-q_3\big) & \text{calculs : on isole } a \text{ et } b \end{array}$$

32 **Question.** Déterminer le pgcd de 19 et 7, ainsi que des coefficients de Bézout.

Nouvelles preuves des résultats précédents

- Avec une relation de Bézout, on peut redémontrer l'inclusion difficile de l'égalité :

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

Allons-y. Prouvons $\subset$.
Considérons une relation de Bézout du type $au + bv = a \wedge b$.
Soit $d \in \mathscr{D}(a) \cap \mathscr{D}(b)$. Alors $d \mid au + bv$. Autrement dit, $d \mid a \wedge b$, c'est-à-dire $d \in \mathscr{D}(a \wedge b)$.

- Avec une relation de Bézout, on peut redémontrer :

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

Allons-y. Montrons une double divisibilité, ce qui suffit car les deux entiers sont dans $\mathbb{N}$, on en déduit qu'ils sont égaux.

— Considérons une relation de Bézout du type $au + bv = a \wedge b$.
Alors $(ka)u + (kb)v = k(a \wedge b)$.
Ainsi (WHY?), $ka \wedge kb \mid k(a \wedge b)$.

— On a $a \wedge b \in \mathscr{D}(a) \cap \mathscr{D}(b)$.
En multipliant par k, on a $k(a \wedge b) \in \mathscr{D}(ka) \cap \mathscr{D}(kb)$.
D'où $k(a \wedge b) \mid ka \wedge kb$.

- Avec une relation de Bézout, on peut redémontrer :

Soit $a, b \in \mathbb{Z}$ et $d = a \wedge b$.
Alors il existe a', b' premiers entre eux tels que $a = da'$ et $b = db'$.

— Si $(a, b) = (0, 0)$, alors $d = 0$. Les entiers $a' = 1$ et $b' = 1$ conviennent.

— Si $(a, b) \neq (0, 0)$, alors $d \neq 0$.
D'une part, comme d est un diviseur de a et b, il existe a', b' tels que $a = da'$ et $b = db'$.
D'autre part, comme $d = \text{pgcd}(a, b)$, le théorème de Bézout fournit $u, v \in \mathbb{Z}$ tel que $au + bv = d$.
En divisant par d, on obtient donc $a'u + b'v = 1$. Ce qui implique d'après le théorème de Bézout que $a' \wedge b' = 1$.

- Avec une relation de Bézout, on peut redémontrer le lemme de Gauss :

Lemme de Gauss. *Soit $a, b, c \in \mathbb{Z}$.*

$$\begin{cases} a \mid bc \\ a \wedge b = 1 \end{cases} \implies a \mid c$$

Écrivons une relation de Bézout entre a et b, disons $au + bv = 1$.
Multiplions-la par c. On obtient $acu + bcv = c$.
Comme $a \mid bc$ (hypothèse), on en déduit que (WHY?) $a \mid acu + bcv$, d'où $a \mid c$.

- Avec une relation de Bézout, on peut redémontrer :

Soit a et $b \in \mathbb{Z}$.
— *Si a et b sont premiers entre eux, alors $a \vee b = |a||b|$*
En particulier :

$$\forall\, m \in \mathbb{Z}, \quad \begin{cases} a \mid m \\ b \mid m \\ a \wedge b = 1 \end{cases} \implies ab \mid m.$$

— *Plus généralement, on a $(a \vee b)(a \wedge b) = |a||b|$.*

Soit $m \in \mathbb{Z}$ tel que $a \mid m$ et $b \mid m$.
Comme $a \wedge b = 1$, on dispose d'une relation de Bézout $au + bv = 1$.
Multiplions-la par m, on a donc $amu + bmv = m$.
Comme $b \mid m$, on a $ab \mid am$. De même $ab \mid bm$.
Par $\mathbb{Z}$-combinaison linéaire, on a $ab \mid m$.

On écrit $a = da'$ et $b = db'$ avec des bonnes notations !

On a alors $(a \wedge b) = d(a' \wedge b') = d$

Encore des conséquences de Bézout

33 **Proposition (nombres premiers entre eux et produit).**
Soit $a, b, c \in \mathbb{Z}$. On a l'implication

$$\begin{cases} a \wedge b = 1 \\ a \wedge c = 1 \end{cases} \implies a \wedge bc = 1$$

« *Si a est premier avec deux entiers, alors a est premier avec leur produit* ».

- **Remarque.** C'est même une équivalence, mais le sens $\impliedby$ est facile, donc presque sans intérêt. Démontrons-le.
  Supposons $a \wedge bc = 1$ et montrons $a \wedge b = 1$ (l'autre égalité est analogue).
  Soit $d \in \mathscr{D}(a) \cap \mathscr{D}(b)$. Alors a fortiori, $d \in \mathscr{D}(a) \cap \mathscr{D}(bc)$, donc $d \mid a \wedge bc$, donc $d \mid 1$.
- **Généralisation.** On a :

$$\begin{cases} a \wedge b_1 = 1 \\ \quad \vdots \\ a \wedge b_r = 1 \end{cases} \implies a \wedge b_1 \cdots b_r = 1$$

- **Généralisation avec puissance.** On a :

$$a \wedge b = 1 \implies \forall \alpha, \beta \in \mathbb{N}, \quad a^\alpha \wedge b^\beta = 1$$

VIII. Congruences (presque HP)

34 **Définition.**
Soit $a, b \in \mathbb{Z}$ et $n \in \mathbb{N}^*$.
On dit que a est congru à b modulo n lorsque $n \mid a - b$.
On écrit $a \equiv b \mod n$.

- **Lien avec la division euclidienne.** Soit $a \in \mathbb{Z}$ et $n \in \mathbb{N}^*$.
  Alors, en notant r le reste de la division euclidienne de a par n, on a $a \equiv r \mod n$.
- **Système de représentants modulo n.**
  Tout nombre $a \in \mathbb{Z}$ est congru modulo $n \in \mathbb{N}^*$ à un unique entier de $\{0, 1, \dots, n-1\}$.
  Par exemple, on a $2024 \equiv ? \mod 3$.

35 **Proposition.**
Soit $n \in \mathbb{N}^*$.
La relation « est congru modulo n » est réflexive, symétrique, transitive.

— Soit $a \in \mathbb{Z}$. On a $a \equiv a \mod n$.

— Soit $a, b \in \mathbb{Z}$ tel que $a \equiv b \mod n$.
Alors $b \equiv a \mod n$.

— Soit $a, b, c \in \mathbb{Z}$ tel que $a \equiv b \mod n$ et $b \equiv c \mod n$.
Alors $a \equiv c \mod n$.

36 **Proposition.**
L'addition et la multiplication de $\mathbb{Z}$ sont compatibles avec la relation de congruence modulo n :

$$\forall\, a, b, c, d \in \mathbb{Z},\quad \begin{cases} a \equiv b \mod n \\ c \equiv d \mod n \end{cases} \implies \Big(a + c \equiv b + d \mod n \quad \text{et} \quad ac \equiv bd \mod n\Big)$$

37 **Proposition (critère de divisibilité de l'école primaire).**
Soit $a \in \mathbb{N}$.

— L'entier a est divisible par 2 si et seulement si son chiffre des unités est 0, 2, 4, 6 ou 8.

— L'entier a est divisible par 3 si et seulement si la somme de ses chiffres est divisible par 3.

— L'entier a est divisible par 4 si et seulement si le nombre obtenu en gardant ses deux derniers chiffres est divisible par 4.

— L'entier a est divisible par 5 si et seulement si son chiffre des unités vaut 0 ou 5.

— L'entier a est divisible par 8 si et seulement si le nombre obtenu en gardant ses trois derniers chiffres est divisible par 8.

— L'entier a est divisible par 9 si et seulement si la somme de ses chiffres est divisible par 9.

— L'entier a est divisible par 10 si et seulement si son chiffre des unités vaut 0.

— L'entier a est divisible par 11 si et seulement si la somme alternée de ses chiffres l'est.

38 **Question.**
Obtenir (à la main !) la décomposition en facteurs premiers de 14 652.

Arithmétique

preuve et éléments de correction

2

Si $d \mid a$, alors $a = kd$. Comme $a \neq 0$, on a $|k| \geqslant 1$. En multipliant par $|d|$, on obtient $a \geqslant |d|$.

6

Première preuve : en exploitant uniquement le fait qu'une partie non vide de $\mathbb{N}$ admet un min.

Unicité. Soit $(q_1, r_1) \in \mathbb{Z}^2$ et $(q_2, r_2) \in \mathbb{Z}^2$ tels que $\begin{cases} a = bq_1 + r_1 \\ 0 \leqslant r_1 < b \end{cases}$ et $\begin{cases} a = bq_2 + r_2 \\ 0 \leqslant r_2 < b. \end{cases}$

Par différence, on a $b(q_1 - q_2) + (r_1 - r_2) = 0$.
Donc $r_1 - r_2 \in b\mathbb{Z}$.
Or $r_1 - r_2 \in]\!]-b, b[\!]$.
On en déduit que $r_1 - r_2 = 0$.
Or $b \neq 0$, donc $q_1 - q_2 = 0$.

Existence.

— **Premier cas :** $a \in \mathbb{N}$
Considérons $E = \{a - kb\}_{k \in \mathbb{N}} \cap \mathbb{N}$.
L'ensemble E est une partie de $\mathbb{N}$ non vide (car $a \in E$).
Donc E admet un plus petit élément.
Posons $r = \min E$.
Comme $r \in E$, l'entier r s'écrit $r = a - bq$ pour un certain $q \in \mathbb{N}$.
On a déjà $r \geqslant 0$. Reste à montrer que $r < b$.
Si on avait $r \geqslant b$, on aurait simultanément $\begin{cases} r - b = a - (q+1)b \\ r - b \in \mathbb{N} \end{cases}$, donc $r - b$ serait dans E.
Or $r - b < r$ (car $b \in \mathbb{N}^*$), et cela contredit la définition de r.

— **Deuxième cas :** $a \in \mathbb{Z} \setminus \mathbb{N}$
On a alors $-a \in \mathbb{N}$.
On applique alors le premier cas. Il existe $(q, r) \in \mathbb{Z}^2$ tel que

$$\begin{cases} (-a) = bq + r \\ 0 \leqslant r < b. \end{cases} \quad \text{c'est-à-dire tel que} \quad \begin{cases} a = b(-q) + (-r) \\ -b < -r \leqslant 0. \end{cases}$$

Si $r = 0$, alors le couple $(-q, 0)$ convient
Si $r \neq 0$, alors $0 < -r + b < b$ et le couple $(-q - 1, -r + b)$ convient.

Deuxième preuve en utilisant qu'une partie de $\mathbb{Z}$ non vide et majorée (dans $\mathbb{Z}$) possède un max.
Notons $E = \{k \in \mathbb{Z} \mid bk \leqslant a\}$.

Analyse. Soit $(q, r) \in \mathbb{Z}^2$ tel que $a = bq + r$ et $0 \leqslant r < b$.
Alors $0 \leqslant a - bq < b$, d'où

$$bq \leqslant a \qquad \text{et} \qquad a < b(q+1)$$

ce qui prouve d'une part que $q \in E$, et que d'autre part pour tout $k > q$, on a $a < bk$, donc $k \notin E$.
Ainsi q apparaît comme étant le maximum de E.
Et r est nécessairement égal à $a - bq$.

Synthèse. L'ensemble E est une partie de $\mathbb{Z}$ non vide et majorée.

— La partie E est non vide.
En effet, $\begin{cases} b0 \leqslant a & \text{si } a \geqslant 0 \\ ba \leqslant a & \text{si } a \leqslant -1 \text{ (car } b \geqslant 1) \end{cases}$ donc $\begin{cases} 0 \in E & \text{si } a \geqslant 0 \\ a \in E & \text{si } a \leqslant -1 \end{cases}$.
Sans disjonction de cas : comme $b \geqslant 1$, on a $b(-|a|) \leqslant -|a| \leqslant a$, donc E contient $-|a|$.

— La partie E est majorée (dans $\mathbb{Z}$). En effet, $\begin{cases} b(a+1) > a & \text{si } a \geqslant 0 \text{ (car } b \geqslant 1) \\ b0 > a & \text{si } a \leqslant -1 \end{cases}$ donc E est majorée par $\begin{cases} a+1 & \text{si } a \geqslant 0 \\ 0 & \text{si } a \leqslant -1 \end{cases}$.
Sans disjonction de cas : comme $b \geqslant 1$, on a $b(|a|+1) > b|a| \geqslant |a| \geqslant a$, donc E est majorée par $|a| + 1$.

Donc E admet un plus grand élément.
Posons $q = \max E$ et $r = a - bq$.
On a alors :

— $bq \leqslant a$, car $q \in E$.

— $a < b(q+1)$, car $q+1 \notin E$.

D'où $bq \leqslant a < b(q+1)$.
En ajoutant $-bq$, on obtient $0 \leqslant a - bq < b$.
D'où $0 \leqslant r < b$.

7

$\boxed{\Longrightarrow}$ Supposons $b \mid a$. Alors il existe $k \in \mathbb{Z}$ tel que $a = bk$.
On a alors :

$$\begin{cases} a = bk + 0 \\ 0 \leqslant 0 < b. \end{cases}$$

Il s'agit donc de la division euclidienne de a par b.
Par unicité de cette division, on en déduit que le reste est nul.

$\boxed{\Longleftarrow}$ Supposons que le reste de la division euclidienne de a par b est nul. Alors la division euclidienne s'écrit $a = bq$. Donc $b \mid a$.

8

• L'ensemble $\mathscr{P}_u$ est une partie de $\mathbb{N}$ (facile), non vide (car u est supposée périodique).
Ainsi, $\mathscr{P}_u$ admet un minimum.
Donc $p_0 = \min \mathscr{P}_u$ est bien défini.

• Montrons l'égalité $\mathscr{P}_u = p_0\mathbb{N}^*$ par double inclusion.
$\boxed{\supset}$ Commençons par cette inclusion (c'est important de commencer par celle-là).
Pour cela, montrons que $\forall\, k \in \mathbb{N}^*,\ p_0 k \in \mathscr{P}_u$.
Procédons par récurrence et pour tout $k \in \mathbb{N}^*$, notons $\mathscr{H}_k$ l'assertion « $p_0 k \in \mathscr{P}_u$ ».

Initialisation. On a $p_0 \in \mathscr{P}_u$, d'où $\mathscr{H}_1$.

Hérédité. Soit $k \in \mathbb{N}^*$ tel que $\mathscr{H}_k$.
Montrons $\mathscr{H}_{k+1}$, c'est-à-dire montrons $\forall\, n \in \mathbb{N},\ u_{n+p_0(k+1)} = u_n$.
Fixons $n \in \mathbb{N}$. On a

$$\begin{array}{lcll} u_{n+p_0(k+1)} & = & u_{(n+p_0k)+p_0} & \text{où } n + p_0 k \in \mathbb{N} \\ & = & u_{n+p_0k} & \text{car } p_0 \in \mathscr{P}_u \\ & = & u_n & \text{d'après } \mathscr{H}_k \end{array}$$

D'où $\mathscr{H}_{k+1}$.

$\boxed{\subset}$ Soit $a \in \mathscr{P}_u$. Montrons que $a \in p_0\mathbb{N}^*$.
Écrivons la division euclidienne de a par p_0 (licite car p_0 est non nul) :
il existe $q, r \in \mathbb{Z}$ tel que $\begin{cases} a = p_0 q + r \\ 0 \leqslant r < p_0 \end{cases}$
Comme $a \in \mathbb{N}$, on en déduit, d'après la remarque portant sur la division euclidienne dans $\mathbb{N}$, que le quotient q est dans $\mathbb{N}$.
On veut montrer que $r = 0$.
Pour cela raisonnons par l'absurde en supposant $r \neq 0$.
On a alors $r \in \mathbb{N}^*$ et montrons que $\forall\, n \in \mathbb{N},\ u_{n+r} = u_n$; ce qui impliquera que $r \in \mathscr{P}_u$.

Soit $n \in \mathbb{N}$.

On a

$$\begin{aligned} u_n &= u_{n+a} \\ &= u_{n+p_0q+r} \\ &= u_{(n+r)+p_0q} \\ &= u_{n+r} \end{aligned}$$

facile si $q=0$, et si $q \in \mathbb{N}^*$, on utilise l'inclusion $\supset$ qui dit que $p_0 q \in \mathscr{P}_u$

On a donc montré que $r \in \mathscr{P}_u$. Or $r < p_0$ (division euclidienne) et $p_0 = \min \mathscr{P}_u$. D'où la contradiction.
On a alors $r = 0$.
Puis $a = p_0 q$.
Comme $a \neq 0$, on a $q \neq 0$, donc $q \in \mathbb{N}^*$.
Bilan : $a \in p_0\mathbb{N}^*$.

11

— Si $(a,b) = (0,0)$, alors $\delta = 0$. Les entiers $a' = 1$ et $b' = 1$ conviennent.

— Sinon, on a en particulier $\delta \geqslant 1$.
Comme δ est un diviseur de a et b, il existe a' et $b' \in \mathbb{Z}$ tels que $a = \delta a'$ et $b = \delta b'$.
Montrons que $\text{pgcd}(a', b') = 1$ en montrant que

$$\forall\, d' \in \mathscr{D}(a') \cap \mathscr{D}(b'), \quad d' \leqslant 1$$

Soit $d' \in \mathscr{D}(a') \cap \mathscr{D}(b')$.
En multipliant par δ, on obtient $d'\delta \in \mathscr{D}(a) \cap \mathscr{D}(b)$. Pour moi : hélas, on ne sait pas encore que $d'\delta \mid a \wedge b = \delta$, sinon on aurait tout de suite $d' \mid 1$.
Par définition du pgcd (en tant que plus grand élément de …), on obtient $d'\delta \leqslant a \wedge b = \delta$.
En divisant par δ (licite car $\delta \geqslant 1$), on obtient $d' \leqslant 1$.

17

— Soit $E = \{d \in [\![2, n]\!] \text{ tel que } d \mid n\} = \mathscr{D}(n) \cap [\![2, +\infty[\![$.
L'ensemble E est une partie de $\mathbb{N}$, non vide ($n \in E$), donc admet un plus petit élément.
Notons $p = \min E$.
On a déjà $p \geqslant 2$ car $p \in E$.
Montrons que p est premier en montrant que $\begin{cases} p \neq 1 \quad \text{(c'est ok)} \\ \mathscr{D}(p) \cap \mathbb{N} = \{1, p\} \end{cases}$
Soit d un diviseur *positif* de p. Supposons $d \neq 1$ et montrons que $d = p$.
Alors par transitivité, on a $d \mid n$.
On a $d \geqslant 2$ donc $d \in E$.
Par définition du minimum de E, on a nécessairement $d \geqslant p$.
Et comme $d \mid p$, on a $d \leqslant p$.
D'où $d = p$.

— Soit $n \geqslant 2$ non premier.
Alors il existe $a, b \in [\![2, n-1]\!]$ tel que $n = ab$.
Quitte à échanger les rôles joués par a et b, on peut supposer que $a \leqslant b$. Ainsi, $a^2 \leqslant n$.
Comme $a \geqslant 2$, on peut trouver un nombre premier p divisant a.
Alors p^2 divise a^2, donc $p^2 \leqslant a^2$. D'où $p^2 \leqslant n$.
D'où $p \leqslant \sqrt{n}$.
On vient de montrer que n possède un diviseur premier p qui est $\leqslant \sqrt{n}$.

20

Soit $d \in \mathbb{N}^*$ un diviseur de n. Écrivons $n = dc$ avec $c \in \mathbb{N}^*$.
Les décompositions en facteurs premiers de n, d et c peuvent s'écrire

$$n = p_1^{\alpha_1} \cdots p_s^{\alpha_s}, \quad d = p_1^{\delta_1} \cdots p_s^{\delta_s} \text{ et } c = p_1^{\gamma_1} \cdots p_s^{\gamma_s}$$

où $p_{r+1}, \dots, p_s$ sont des nombres premiers distincts, et différents de $p_1, \dots, p_r$.
De l'égalité $n = dc$ et par unicité de la décomposition en facteurs premiers, on a :

— pour tout $i \in [\![1, r]\!]$, $\alpha_i = \delta_i + \gamma_i$, d'où $\delta_i \in [\![0, \alpha_i]\!]$;
— pour tout $i \in [\![r+1, s]\!]$, $0 = \delta_i + \gamma_i$, d'où, par positivité, $\delta_i = 0$ (et $\gamma_i = 0$).

On en déduit que $d = p_1^{\delta_1} \cdots p_r^{\delta_r}$.

22

Notons $d = \prod_{i=1}^{r} p_i^{\min(\alpha_i, \beta_i)}$.
Il s'agit de montrer que d est le plus grand élément de $\mathscr{D}(a) \cap \mathscr{D}(b)$.

— Montrons que d est un diviseur commun à a et b.
Montrons d'abord que $d \mid a$.
D'après la proposition précédente 20, il s'agit de montrer que

$$\forall\, i \in [\![1, r]\!],\ \min(\alpha_i, \beta_i) \leqslant \alpha_i$$

ce qui est évident.

On montre de même que $d \mid b$.

— Soit $d' \in \mathscr{D}(a) \cap \mathscr{D}(b)$. Montrons que $d' \leqslant d$.
D'après la proposition précédente 20, d' a une décomposition du type $d' = p_1^{\delta_1} \cdots p_r^{\delta_r}$ avec

$$\forall\, i \in [\![1, r]\!],\ \begin{cases} \delta_i \in [\![0, \alpha_i]\!] & \text{car } d \mid a \\ \delta_i \in [\![0, \beta_i]\!] & \text{car } d \mid b \end{cases} \qquad \text{donc avec} \qquad \forall\, i \in [\![1, r]\!],\ \delta_i \in [\![0, \min(\alpha_i, \beta_i)]\!]$$

On a alors directement $d' \leqslant d$.

23

— Il suffit de prouver cette formule pour $a, b \in \mathbb{N}$ (car elle est invariante par $a \leftrightarrow b$ et par $a \leftrightarrow -a$ (et donc par $b \leftrightarrow -b$)).
— Le cas $\big(a = 0 \text{ ou } b = 0\big)$ est facile et résulte du fait que, dans ce cas, $\operatorname{ppcm}(a, b) = 0$.
— Le cas où $a, b \in \mathbb{N}^*$ repose sur la proposition 22 et le fait que $\min(\alpha, \beta) + \max(\alpha, \beta) = \alpha + \beta$.
Comme a et b sont dans $\mathbb{N}^*$, on peut considérer leur décomposition en facteurs premiers, disons

$$a = p_1^{\alpha_1} \cdots p_r^{\alpha_r} \quad \text{et} \quad b = p_1^{\beta_1} \cdots p_r^{\beta_r}$$

On a alors :

$$\begin{aligned}
\operatorname{pgcd}(a, b) \times \operatorname{ppcm}(a, b) &= \prod_{i=1}^{r} p_i^{\min(\alpha_i, \beta_i)} \times \prod_{i=1}^{r} p_i^{\max(\alpha_i, \beta_i)} && \text{d'après 22} \\
&= \prod_{i=1}^{r} p_i^{\min(\alpha_i, \beta_i) + \max(\alpha_i, \beta_i)} && \text{calcul sur les puissances} \\
&= \prod_{i=1}^{r} p_i^{\alpha_i + \beta_i} && \text{définition du min et du max} \\
&= \prod_{i=1}^{r} p_i^{\alpha_i} \times \prod_{i=1}^{r} p_i^{\beta_i} && \text{calcul sur les puissances} \\
&= ab
\end{aligned}$$

24

• Commençons par le cas $b \in \mathbb{N}$.
Par récurrence. Notons $\mathscr{H}_b$ la propriété « Pour tout $a \in \mathbb{Z}$, on a $\mathscr{D}(a) \cap \mathscr{D}(b) = \mathscr{D}(a \wedge b)$ ».

Initialisation.

Soit $a \in \mathbb{Z}$.

D'une part, on a $\mathscr{D}(a) \cap \mathscr{D}(0) = \mathscr{D}(a) \cap \mathbb{Z} = \mathscr{D}(a)$; d'autre part, $a \wedge b = a \wedge 0 = a$.

D'où $\mathscr{H}_0$.

Hérédité. Soit $b \in \mathbb{N}^*$. On suppose que $\mathscr{H}_r$ est vraie pour tout $r \in [\![0, b-1]\!]$.

Montrons $\mathscr{H}_b$.

Soit $a \in \mathbb{Z}$. Écrivons la division euclidienne $a = bq + r$, licite car $b \in \mathbb{N}^*$.

D'après $\mathscr{H}_r$ (la $\forall$-assertion est appliquée à b), on a $\mathscr{D}(b) \cap \mathscr{D}(r) = \mathscr{D}(b \wedge r)$.

D'après le lemme fondamental (ne nécessitant aucune hypothèse sur b et r), on a $\mathscr{D}(a) \cap \mathscr{D}(b) = \mathscr{D}(b) \cap \mathscr{D}(r)$ et $a \wedge b = b \wedge r$.

Il n'y a plus qu'à remplacer : on obtient $\mathscr{D}(a) \cap \mathscr{D}(b) = \mathscr{D}(a \wedge b)$.

D'où $\mathscr{H}_b$.

• Traitons le cas $b \in \mathbb{Z} \setminus \mathbb{N}$.
Alors $-b \in \mathbb{N}$. Donc d'après le cas précédent, $\mathscr{D}(a) \cap \mathscr{D}(-b) = \mathscr{D}(a \wedge -b)$.
Or $\mathscr{D}(-b) = \mathscr{D}(b)$ et $a \wedge -b = a \wedge b$, d'où le résultat.

25

Prouvons l'inclusion difficile $a\mathbb{Z} \cap b\mathbb{Z} \subset (a \vee b)\mathbb{Z}$.
Le cas où a ou b est nul est immédiat.
Supposons désormais a et b non nuls.
Posons $\mu = a \vee b \geqslant 1$.
Soit $m \in a\mathbb{Z} \cap b\mathbb{Z}$.
Effectuons la division euclidienne de m par μ. On a $m = \mu q + r$ avec $0 \leqslant r < \mu$.
Comme $r = m - \mu q$ et que $m, \mu \in a\mathbb{Z} \cap b\mathbb{Z}$, on a alors $r \in a\mathbb{Z} \cap b\mathbb{Z}$.
Si $r \neq 0$, alors r serait dans $a\mathbb{Z} \cap b\mathbb{Z} \cap \mathbb{N}^*$ et plus petit que le minimum de cet ensemble, à savoir μ.
Ce qui n'est pas possible.
Donc $r = 0$.
Donc $r = \mu q$. Donc $r \in \mu\mathbb{Z}$.

26

Cas $k = 0$. C'est facile.
Cas $k \neq 0$**.** On va utiliser la caractérisation du pgcd, cf. 24, grâce à la reformulation avec l'équivalence.
On a $k \in \mathscr{D}(ka) \cap \mathscr{D}(kb)$, donc avec 24, on a $k \in \mathscr{D}(ka \wedge kb)$.
Ainsi, on peut trouver d tel que $ka \wedge kb = kd$. Il s'agit de montrer que $d = a \wedge b$.
D'après 24, on a $\mathscr{D}(kd) = \mathscr{D}(ka) \cap \mathscr{D}(kb)$.
Comme $k \neq 0$, on peut simplifier par k et on obtient $\mathscr{D}(d) = \mathscr{D}(a) \cap \mathscr{D}(b)$.
Donc $d = a \wedge b$.

27

On a $a \in \mathscr{D}(ac) \cap \mathscr{D}(bc)$ (une appartenance est automatique, l'autre résulte de l'hypothèse).
D'après la caractérisation 24, on en déduit $a \in \mathscr{D}(ac \wedge bc)$.
Or $ac \wedge bc = c(a \wedge b)$, d'après 26.
L'hypothèse $a \wedge b = 1$ fournit donc $ac \wedge bc = c$.
D'où $a \in \mathscr{D}(c)$.

30

• Commençons par le cas $b \in \mathbb{N}$.
Par récurrence. Notons $\mathscr{H}_b$ la propriété « Pour tout $a \in \mathbb{Z}$, il existe $u, v \in \mathbb{Z}$ tel que $au + bv = a \wedge b$ ».

Initialisation.

Soit $a \in \mathbb{Z}$.

On a $a \wedge b = a \wedge 0 = |a|$.

Si $a \in \mathbb{N}$, alors $a \times 1 + b \times 0 = |a| = a \wedge b$.

Si $a \in \mathbb{Z} \setminus \mathbb{N}$, alors $a \times (-1) + b \times 0 = |a| = a \wedge b$.

D'où $\mathscr{H}_0$.

Hérédité. Soit $b \in \mathbb{N}^*$. On suppose que $\mathscr{H}_r$ est vraie pour tout $r \in [\![0, b-1]\!]$.

Montrons $\mathscr{H}_b$.

Soit $a \in \mathbb{Z}$. Écrivons la division euclidienne $a = bq + r$.

D'après $\mathscr{H}_r$ (la $\forall$-assertion est appliquée à $b \in \mathbb{Z}$), il existe $u, v \in \mathbb{Z}$ tel que $bu + rv = b \wedge r$.

D'après le lemme fondamental (ne nécessitant aucune hypothèse sur b et r), on a $b \wedge r = a \wedge b$.

Il n'y a plus qu'à remplacer tous les (b, r) par (a, b) : on obtient $bu + (a - bq)v = a \wedge b$.

En réagençant, on obtient $av + b(u - qv) = a \wedge b$.

D'où $\mathscr{H}_b$.

• Traitons le cas $b \in \mathbb{Z} \setminus \mathbb{N}$.
Alors $-b \in \mathbb{N}$. Donc d'après le cas précédent, il existe u, v tel que $au + (-b)v = \text{pgcd}(a, -b)$.
D'après le cours, on a $\text{pgcd}(a, -b) = \text{pgcd}(a, b)$.
On en déduit $au + b(-v) = \text{pgcd}(a, b)$.
On a donc obtenu une relation de Bézout entre a et b.

Pour la deuxième partie.
$\boxed{\Longrightarrow}$ C'est un cas particulier du point précédent.
$\boxed{\Longleftarrow}$ Soit $d \in \mathscr{D}(a) \cap \mathscr{D}(b)$. Alors $d \mid au + bv$, donc $d \mid 1$. Donc $a \wedge b = 1$.