CHAPITRE N°12
ARITHMÉTIQUE DANS $\mathbb{Z}$

§ 1 RELATION BINAIRE SUR UN ENSEMBLE

C12.1. DÉFINITION (RELATION BINAIRE SUR UN ENSEMBLE) Soit E un ensemble.

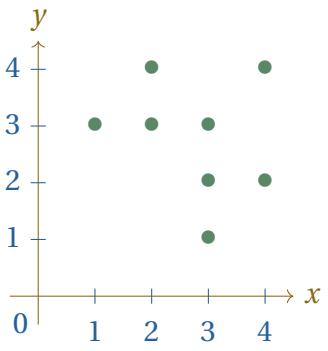
1. Une relation binaire sur E est une partie $\mathscr{R}$ de $E \times E$.
2. Soient $\mathscr{R}$ une relation binaire sur E et $(x, y) \in E^2$. On dit que x est en relation avec y et on écrit $x \mathscr{R} y$ si $(x, y) \in \mathscr{R}$.

C12.2. EXEMPLE DE RELATION BINAIRE SUR $E = [\![1, 4]\!]$

L'ensemble $\mathscr{R}$ défini par :

$$\mathscr{R} = \{(1,3), (3,1), (2,3), (2,4), (3,3), (3,2), (4,2), (4,4)\}$$

est une relation binaire sur l'ensemble $E = [\![1, 4]\!]$.



C12.3. DÉFINITION (TERMINOLOGIE ASSOCIÉE À UNE RELATION BINAIRE) Soit E un ensemble muni d'une relation binaire $\mathscr{R}$.

1. La relation $\mathscr{R}$ est dite réflexive si $\forall (x, y) \in E^2 \quad x \mathscr{R} x.$
2. La relation $\mathscr{R}$ est dite symétrique si $\forall (x, y) \in E^2 \quad x \mathscr{R} y \Longrightarrow y \mathscr{R} x.$
3. La relation $\mathscr{R}$ est dite antisymétrique si $\forall (x, y) \in E^2 \quad \big(x \mathscr{R} y \text{ et } y \mathscr{R} x\big) \Longrightarrow x = y.$
4. La relation $\mathscr{R}$ est dite transitive si $\forall (x, y, z) \in E^3 \quad \big(x \mathscr{R} y \text{ et } y \mathscr{R} z\big) \Longrightarrow x \mathscr{R} z.$

C12.4. DÉFINITION (RELATION D'ORDRE) Soit E un ensemble.

1. Une relation d'ordre sur E est une relation binaire $\mathscr{R}$ telle que :

   $\mathscr{R}$ est réflexive, antisymétrique, et transitive.

2. Une relation d'ordre $\mathscr{R}$ sur E est dite totale si $\forall (x, y) \in E^2 \quad x \mathscr{R} y \text{ ou } y \mathscr{R} x.$ Elle est dite partielle dans le cas contraire.

C12.5. Exemple (relation d'ordre $\subset$ sur $\mathscr{P}(E)$) Soit E un ensemble. La relation d'inclusion $\subset$ sur $\mathscr{P}(E)$ est une relation d'ordre sur $\mathscr{P}(E)$. Elle est partielle dès que E possède deux éléments distincts et totale lorsque E est l'ensemble vide ou un singleton.

C12.6. Définition (relation d'équivalence) Soit E un ensemble. Une relation d'équivalence sur E est une relation binaire $\mathscr{R}$ telle que :

$\mathscr{R}$ est réflexive, symétrique, et transitive.

C12.7. Exemple (relation d'équivalence sur $\mathbb{C}$)) La relation $\mathscr{R}$ définie sur $\mathbb{C}$ par :

$$\forall (z_1, z_2) \in \mathbb{C}^2 \quad z_1 \mathscr{R} z_2 :\iff z_1^2 = z_2^2$$

est une relation d'équivalence sur $\mathbb{C}$.

C12.8. Définition (classe d'équivalence) Soient E un ensemble muni d'une relation d'équivalence $\mathscr{R}$ et $x \in E$. La classe d'équivalence de x notée $\overline{x}$ est la partie de E définie par :

$$\overline{x} = \{y \in E \,:\, x \mathscr{R} y\}\,.$$

C12.9. Exercice Soient E un ensemble muni d'une relation d'équivalence $\mathscr{R}$ et $(x, y) \in E^2$. Démontrer que $x \mathscr{R} y$ si et seulement si $\overline{x} = \overline{y}$.

C12.10. Exercice (relation d'équivalence sur $\mathbb{C}^*$)

1. Démontrer que la relation $\mathscr{R}$ définie sur $\mathbb{C}^*$ par :
$$\forall (z_1, z_2) \in \mathbb{C}^* \times \mathbb{C}^* \quad z_1 \mathscr{R} z_2 :\iff \frac{z_1}{z_2} \in \mathbb{R}_{>0}$$
est une relation d'équivalence sur $\mathbb{C}^*$.
2. Déterminer la classe d'équivalence d'un élément $z \in \mathbb{C}^*$ et la représenter graphiquement.
3. Quelle propriété remarquable possèdent l'ensemble des classes d'équivalences ici ?

C12.11. Propriété (les classes d'équivalence forment une partition) Soit E un ensemble muni d'une relation d'équivalence $\mathscr{R}$. Soit $\mathscr{E}$ l'ensemble des classes d'équivalence de $\mathscr{R}$.

L'ensemble $\mathscr{E}$ des classes d'équivalence de $\mathscr{R}$ forme une partition de E

i.e. :

1. $\forall (C_1, C_2) \in \mathscr{E}^2 \quad C_1 \neq C_2 \implies C_1 \cap \mathbb{C}_2 = \emptyset$;
2. $\bigcup_{C \in \mathscr{E}} C = E$.

C12.12. Exercice Démontrer que la relation $\mathscr{R}$ définie sur $\mathbb{C}$ par :

$$\forall (z_1, z_2) \in \mathbb{C} \times \mathbb{C} \quad z_1 \mathscr{R} z_2 :\iff |z_1| = |z_2|$$

est une relation d'équivalence sur $\mathbb{C}$ et décrire ses classes d'équivalence.

C12.13. Exercice Soit $(C_i)_{i \in I}$ une partition d'un ensemble E. Construire une relation $\mathscr{R}$ sur E dont les classes d'équivalences sont les C_i $(i \in I)$.

§ 2 Divisibilité et division euclidienne

C12.14. Définition (divisibilité dans $\mathbb{Z}$) Soit $(a,b) \in \mathbb{Z}^2$. On dit que :

a divise b ou b est divisible par a ou b est un multiple de a

et on note $a \mid b$ si $\boxed{\exists q \in \mathbb{Z} \quad b = qa.}$

C12.15. Remarque

1. La relation de divisibilité sur $\mathbb{Z}$ est réflexive, transitive, mais n'est ni symétrique, ni antisymétrique.
2. La relation de divisibilité sur $\mathbb{N}$ est une relation d'ordre.

C12.16. Définition (couple d'entiers associés) Soit $(a,b) \in \mathbb{Z}^2$. On dit que les entiers a et b sont associés si $a \mid b$ et $b \mid a$.

C12.17. Remarque La relation $\mathscr{R}$ sur $\mathbb{Z}$ définie par, pour tout $(a,b) \in \mathbb{Z}^2$, $a \mathscr{R} b$ si et seulement si a et b sont associés est une relation d'équivalence sur $\mathbb{Z}$.

C12.18. Proposition (caractérisation des entiers associés) Soit $(a,b) \in \mathbb{Z}^2$. Les entiers a et b sont associés si et seulement si $a = b$ ou $a = -b$.

C12.19. Théorème (division euclidienne dans $\mathbb{Z}$) Soit $(a,b) \in \mathbb{Z} \times \mathbb{N}^*$.

$$\boxed{\exists!\,(q,r) \in \mathbb{Z} \times [\![0, b-1]\!] \quad a = bq + r\,.}$$

Le nombre q (resp. r) est appelé quotient (resp. reste) de la division euclidienne de a par b.

C12.20. Exercice Construire une fonction Python **division** d'arguments :

- **a** un entier relatif ;
- **b** un entier naturel non nul ;

qui renvoie le couple **(q, r)** formé par la quotient et le reste de la division euclidienne de a par b.

C12.21. Exercice Déterminer le quotient et le reste de la division euclidienne de 12 345 par 29.

C12.22. Proposition (critère de divisibilité) Soit $(a,b) \in \mathbb{Z} \times \mathbb{N}^*$. Alors $a \mid b$ si et seulement si le reste de la division euclidienne de b par a est nul.

§ 3 PGCD ET ALGORITHME D'EUCLIDE

C12.23. DÉFINITION (ENSEMBLE DES DIVISEURS POSITIFS D'UN ENTIER)
Soit $a \in \mathbb{Z}$. On note $\mathrm{Div}(a)$ l'ensemble des diviseurs positifs de a.

C12.24. LEMME (CARDINAL DE L'ENSEMBLE DES DIVISEURS POSITIFS D'UN ENTIER NATUREL)
1. $\mathrm{Div}(0) = \mathbb{N}$
2. Si $a \in \mathbb{N}^*$ alors $\{1, a\} \subset \mathrm{Div}(a) \subset [\![1, a]\!]$ et donc $\mathrm{Div}(a)$ est une partie finie non vide de $\mathbb{N}$.

C12.25. DÉFINITION (PGCD DE DEUX ENTIERS NATURELS NON TOUS LES DEUX NULS)
Soient a et b deux entiers naturels non tous les deux nuls. Le Plus Grand Commun Diviseur (PGCD) de a et b, noté $a \wedge b$, est défini par $\boxed{a \wedge b = \max(\mathrm{Div}(a) \cap \mathrm{Div}(b))}$ où le max est relatif à la relation d'ordre $\leqslant$ usuelle sur $\mathbb{N}$.

C12.26. EXERCICE Soit $a \in \mathbb{N}^*$. Déterminer $a \wedge 0$, $a \wedge 1$ et $a \wedge a$.

C12.27. PROPOSITION Si $b \in \mathbb{N}^*$ est un diviseur de $a \in \mathbb{N}$ alors :

$$\mathrm{Div}(b) \subset \mathrm{Div}(a) \quad ; \quad \mathrm{Div}(a) \cap \mathrm{Div}(b) = \mathrm{Div}(b) \quad ; \quad a \wedge b = b\,.$$

Démonstration

- Soit $d \in \mathrm{Div}(b)$. Comme $d \mid b$ et $b \mid a$ il vient $d \mid a$ (transitivité de la relation d'ordre $\mid$ sur $\mathbb{N}$). Ainsi $d \in \mathrm{Div}(a)$.
- De $\mathrm{Div}(b) \subset \mathrm{Div}(a)$ on déduit :

$$\underbrace{\mathrm{Div}(b) \cap \mathrm{Div}(b)}_{\mathrm{Div}(b)} \subset \mathrm{Div}(a) \cap \mathrm{Div}(b)\,.$$

Avec $\mathrm{Div}(a) \cap \mathrm{Div}(b) \subset \mathrm{Div}(b)$, il vient $\mathrm{Div}(a) \cap \mathrm{Div}(b) = \mathrm{Div}(b)$.

- En prenant le maximum (pour la relation d'ordre $\leqslant$ sur $\mathbb{N}$), nous déduisons de $\mathrm{Div}(a) \cap \mathrm{Div}(b) = \mathrm{Div}(b)$:

$$a \wedge b = \max(\mathrm{Div}(a) \cap \mathrm{Div}(b)) = \max(\mathrm{Div}(b))\,.$$

Comme b est le plus grand diviseur de b, $a \wedge b = \max(\mathrm{Div}(b)) = b$.

C12.28. EXERCICE Déterminer $770 \wedge 1050$.

C12.29. LEMME (CLÉ POUR L'ALGORITHME D'EUCLIDE) Soit $(a, b) \in \mathbb{N}^2$ tel que $1 \leqslant b < a$.
Soit $q \in \mathbb{N}$ (resp. $r \in [\![0, b-1]\!]$) le quotient (rep. reste) de la division euclidienne de a par b, de sorte que $a = bq + r$.

$$\boxed{\mathrm{Div}(a) \cap \mathrm{Div}(b) = \mathrm{Div}(b) \cap \mathrm{Div}(r) \quad \text{et} \quad a \wedge b = b \wedge r\,.}$$

Démonstration

⊂ Soit $d \in \mathrm{Div}(a) \cap \mathrm{Div}(b)$. Alors il existe $(\alpha, \beta) \in \mathbb{N}^2$ tel que $a = d\alpha$ et $b = d\beta$. Comme :

$$r = a - bq = d \cdot \underbrace{(\alpha - \beta q)}_{\in \mathbb{Z}}$$

il vient $d \in \mathrm{Div}(r)$. Ainsi $d \in \mathrm{Div}(b) \cap \mathrm{Div}(r)$. Donc $\mathrm{Div}(a) \cap \mathrm{Div}(b) \subset \mathrm{Div}(b) \cap \mathrm{Div}(r)$.

⊃ Soit $d \in \mathrm{Div}(b) \cap \mathrm{Div}(r)$. Alors il existe $(\beta, \rho) \in \mathbb{N}^2$ tel que $b = d\beta$ et $r = d\rho$. Comme :

$$a = bq + r = d \cdot \underbrace{(\beta q + \rho)}_{\in \mathbb{Z}}$$

il vient $d \in \mathrm{Div}(a)$. Ainsi $d \in \mathrm{Div}(a) \cap \mathrm{Div}(b)$. Donc $\mathrm{Div}(b) \cap \mathrm{Div}(r) \subset \mathrm{Div}(a) \cap \mathrm{Div}(b)$.

- De $\mathrm{Div}(a) \cap \mathrm{Div}(b) = \mathrm{Div}(b) \cap \mathrm{Div}(r)$ nous déduisons :

$$a \wedge b = \max(\mathrm{Div}(a) \cap \mathrm{Div}(b)) = \max(\mathrm{Div}(b) \cap \mathrm{Div}(r)) = b \wedge r \,.$$

C12.30. Algorithme d'Euclide Soit $(a, b) \in \mathbb{N}^2$ tel que $1 \leqslant b < a$. On définit des entiers naturels $a_0, a_1, \ldots$ et $b_0, b_1, \ldots$ comme suit.

- On pose $a_0 = a$ et $b_0 = b$.
- pour tout $k \in \mathbb{N}$, si $b_k = 0$ alors la construction s'arrête, sinon elle se poursuit et on pose :

$$a_{k+1} = b_k \quad , \quad b_{k+1} = \text{reste de la division euclidienne de } a_k \text{ par } b_k \quad [\text{donc } b_{k+1} < b_k] \,.$$

Alors on a les propriétés suivantes.

1. La construction des entiers $a_0, a_1, \ldots$ et $b_0, b_1, \ldots$ s'arrête au bout d'un nombre fini d'étapes.
2. Si n est le rang des derniers entiers a_k et b_k construits, alors $n \geqslant 1$ et $b = b_0 > b_1 > \ldots > b_n = 0$.
3. $\mathrm{Div}(a) \cap \mathrm{Div}(b) = \mathrm{Div}(b_{n-1})$ et $a \wedge b = b_{n-1}$

Démonstration

1. Raisonnons par l'absurde, et supposons que la construction ne s'arrête pas. Dans ce cas, pour tout $k \in \mathbb{N}$, l'entier naturel b_k est construit. Nous disposons donc d'une suite $(b_k)_{k \in \mathbb{N}}$ d'entiers naturels strictement décroissante. Contradiction.

2. Comme l'entier $b_0 = b$ est non nul, les entiers a_1 et b_1 sont construits. donc $n \geqslant 1$. Par définition même des entiers $b = b_0, b_1, \ldots, b_n$ on a $b = b_0 > b_1 > \ldots > b_n$. Comme les entiers a_{n+1} et b_{n+1} ne sont pas construits, $b_n = 0$.

3. Pour tout $k \in [\![0, n-1]\!]$, $a_{k+1} = b_k$ et b_{k+1} est le reste de la division euclidienne de a_k par b_k. Grâce à C12.29 :

$$\mathrm{Div}(a_k) \cap \mathrm{Div}(b_k) = \mathrm{Div}(b_k) \cap \mathrm{Div}(b_{k+1}) = \mathrm{Div}(a_{k+1}) \cap \mathrm{Div}(b_{k+1})$$

et donc :

$$(\star) \qquad \underbrace{\mathrm{Div}(a_0) \cap \mathrm{Div}(b_0)}_{\mathrm{Div}(a) \cap \mathrm{Div}(b)} = \mathrm{Div}(a_1) \cap \mathrm{Div}(b_1) = \ldots = \mathrm{Div}(a_{n-1}) \cap \mathrm{Div}(b_{n-1}) \,.$$

Comme $b_n = 0$ est le reste de la division euclidienne de a_{n-1} par b_{n-1}, b_{n-1} divise a_{n-1}. D'après C12.27 :

$$(\star\star) \qquad \mathrm{Div}(a_{n-1}) \cap \mathrm{Div}(b_{n-1}) = \mathrm{Div}(b_{n-1}) \,.$$

De $(\star)$ et $(\star\star)$ on déduit $\mathrm{Div}(a) \cap \mathrm{Div}(b) = \mathrm{Div}(b_{n-1})$ puis :

$$a \wedge b = \max(\mathrm{Div}(a) \cap \mathrm{Div}(b)) = \max(\mathrm{Div}(b_{n-1})) = b_{n-1} \,.$$

C12.31. Exemple Nous calculons $255 \wedge 141$ au moyen de l'algorithme d'Euclide.

Étape	Division euclidienne de a_k par b_k	Valeur de a_k	Valeur de b_k
0		$a_0 = 255$	$b_0 = 141$
1	$\underbrace{255}_{a_0} = 1 \cdot \underbrace{141}_{b_0} + \underbrace{114}_{\text{reste n°1}}$	$a_1 = b_0 = 141$	$b_1 = \text{reste n°1} = 114$
2	$\underbrace{141}_{a_1} = 1 \cdot \underbrace{114}_{b_1} + \underbrace{27}_{\text{reste n°2}}$	$a_2 = b_1 = 114$	$b_2 = \text{reste n°2} = 27$
3	$\underbrace{114}_{a_2} = 4 \cdot \underbrace{27}_{b_2} + \underbrace{6}_{\text{reste n°3}}$	$a_3 = b_2 = 27$	$b_3 = \text{reste n°3} = 6$
4	$\underbrace{27}_{a_3} = 4 \cdot \underbrace{6}_{b_3} + \underbrace{3}_{\text{reste n°4}}$	$a_4 = b_3 = 6$	$\underbrace{b_4 = \text{reste n°4} = 3}_{\text{dernier reste non nul}}$
5	$\underbrace{6}_{a_4} = 2 \cdot \underbrace{3}_{b_4} + \underbrace{0}_{\text{reste n°5}}$	$a_5 = b_4 = 3$	$b_5 = \text{reste n°5} = 0$

Nous en déduisons $255 \wedge 141 = 3$.

C12.32. Corollaire $(a, b) \in \mathbb{N}^2$ tels que $1 \leqslant b < a$.

$$\text{Div}(a) \cap \text{Div}(b) = \text{Div}(a \wedge b)$$

Démonstration Il s'agit simplement d'assembler les deux résultats du 3 de C12.30.

C12.33. Exemple L'ensemble des entiers naturels n divisant 1 234 et 5 678 est $\{1, 2\}$.
En effet, l'algorithme d'Euclide permet de calculer $1\,234 \wedge 5\,678 = 2$. D'après C12.32 un entier naturel n divise 1 234 et 5 678 si et seulement s'il divise 2.

C12.34. Exercice Construire une fonction Python **pgcd** d'arguments :

- **a** un entier naturel non nul ;
- **b** un entier naturel non nul ;

qui renvoie le PGCD de **a** et **b** en implémentant l'algorithme d'Euclide.

C12.35. Proposition (PGCD de deux entiers naturels multiples d'un même nombre)
Soient $(a,b) \in \mathbb{N}^2$ tels que $1 \leqslant b < a$ et $k \in \mathbb{N}^*$.

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

Démonstration

Notons :

- n le nombre de divisions euclidiennes effectués pour calculer $a \wedge b$ avec l'algorithme d'Euclide ;
- $a_0, \dots, a_n$ et $b_0 > \dots > b_{n-1} = a \wedge b > b_n = 0$ les entiers construits lors de l'exécution de l'algorithme d'Euclide pour calculer $a \wedge b$;
- $a'_0, a'_1, \dots$ et $b'_0, b'_1, \dots$ les entiers construits lors de l'exécution de l'algorithme d'Euclide pour calculer $(ka) \wedge (kb)$.

Nous démontrons que pour tout $\ell \in [\![0, n]\!]$, $a'_\ell = k \cdot a_\ell$ et $b'_\ell = k \cdot b_\ell$.

— *Initialisation* Par définition $a'_0 = k \cdot a = k \cdot a_0$ et $b'_0 = k \cdot b = k \cdot b_0$.

— *Hérédité* Soit $\ell \in [\![0, n-1]\!]$ tel que $a'_\ell = k \cdot a_\ell$ et $b'_\ell = k \cdot b_\ell$.

. Comme $b_\ell \neq 0$, $a_{\ell+1} = b_\ell$ et $b_{\ell+1}$ est le reste de la division euclidienne de a_ℓ par b_ℓ, i.e. :

$$b_{\ell+1} \in [\![0, b_\ell - 1]\!] \text{ et il existe } q_\ell \in \mathbb{Z} \text{ tel que } a_\ell = q_\ell \cdot b_\ell + b_{\ell+1}$$

et donc :

$$k \cdot b_{\ell+1} \in [\![0, k \cdot b_\ell - k]\!] \subset [\![0, k \cdot b_\ell - 1]\!] \text{ et } k \cdot a_\ell = q_\ell \cdot k \cdot b_\ell + k \cdot b_{\ell+1}\,.$$

identité qui s'écrit encore, grâce à l'hypothèse de récurrence :

$$(\star) \qquad k \cdot b_{\ell+1} \in [\![0, b'_\ell - 1]\!] \text{ et } a'_\ell = q_\ell \cdot b'_\ell + k \cdot b_{\ell+1}\,.$$

. Comme $b'_\ell = k \cdot b_\ell \neq 0$, $a'_{\ell+1} = b'_\ell = k \cdot b_\ell = k \cdot a_{\ell+1}$ et $b'_{\ell+1}$ est le reste de la division euclidienne de a'_ℓ par b'_ℓ. D'après $(\star)$, $b'_{\ell+1} = k \cdot b_{\ell+1}$.

Avec la récurrence finie précédente, il vient :

$$b'_{n-1} = k \cdot b_{n-1} \geqslant 1 \qquad \text{et} \qquad b'_n = k \cdot b_n = 0\,.$$

D'après C12.30 :

$$(k \cdot a) \wedge (k \cdot b) = b'_{n-1} = k \cdot b_{n-1} = k \cdot (a \wedge b)\,.$$

C12.35.01. Exemple $48 \wedge 80 = (16 \cdot 3) \wedge (16 \cdot 5) = 16 \cdot (3 \wedge 5) = 16$

C12.36. Corollaire Soient a et b deux entiers naturels non tous les deux nuls. Alors :

$a \wedge b$ est le plus grand élément de $\mathrm{Div}(a) \cap \mathrm{Div}(b)$ pour la relation d'ordre $\mid$ sur $\mathbb{N}$.

i.e. :

- $a \wedge b \mid a$ et $a \wedge b \mid b$;
- $\forall\, d \in \mathbb{N} \quad (d \mid a \text{ et } d \mid b) \implies d \mid a \wedge b$;

Démonstration

- Par définition du PGCD de a et b, $a \wedge b$ divise a et b.
- Soit d un entier naturel divisant a et b. D'après C12.32 :

$$d \in \mathrm{Div}(a) \cap \mathrm{Div}(b) = \mathrm{Div}(a \wedge b)$$

et donc d divise $a \wedge b$.

C12.37. Définition (PGCD de deux entiers relatifs)
Soient $(a,b) \in \mathbb{Z}^2$. Le Plus Grand Commun Diviseur (PGCD) de a et b, noté $a \wedge b$, est défini par :

$a \wedge b$ est le plus grand entier naturel, pour la relation d'ordre $\mid$ sur $\mathbb{N}$, qui divise a et b.

C12.38. Remarques

- La définition C12.37 étend la définition C12.25, cf. C12.36.
- Avec la définition C12.37, $0 \wedge 0 = 0$.
- Pour tout $(a,b) \in \mathbb{Z}^2$, $a \wedge b = |a| \wedge |b|$.

C12.39. Proposition (relation de Bézout) Soient a et b deux entiers relatifs.

$$\exists (u,v) \in \mathbb{Z}^2 \quad au + bv = a \wedge b \qquad \text{[relation de Bézout]}\ .$$

Démonstration

Nous supposons $1 \leqslant b < a$ et nous notons :

- n le nombre de divisions euclidiennes effectués pour calculer $a \wedge b$ avec l'algorithme d'Euclide ;
- $a_0, \dots, a_n$ et $b_0 > \dots > b_{n-1} = a \wedge b > b_n = 0$ les entiers construits lors de l'exécution de l'algorithme d'Euclide pour calculer $a \wedge b$.

Nous supposons $n \geqslant 2$ (le cas où $n = 1$ est facile car alors b divise a) et nous démontrons que, pour tout $k \in [\![0, n-2]\!]$:

$$\exists (u_k, v_k) \in \mathbb{Z}^2 \quad a_k u_k + b_k v_k = a \wedge b$$

par récurrence descendante finie.

— *Initialisation au rang $n-2$* $b_{n-1} = a \wedge b$ est le reste de la division euclidienne de a_{n-2} par b_{n-2}. Donc il existe $q_{n-2} \in \mathbb{Z}$ tel que $a_{n_2} = b_{n-2} q_{n-2} + a \wedge b$ et donc :

$$a_{n-2} \cdot \underbrace{1}_{u_{n-2} \in \mathbb{Z}} + b_{n-2} \cdot \underbrace{(-q_{n-2})}_{v_{n-2} \in \mathbb{Z}} = a \wedge b\,.$$

— *Hérédité* Soit $k \in [\![1, n-2]\!]$ tel qu'il existe $(u_k, v_k) \in \mathbb{Z}^2$ vérifiant :

$$(\star) \qquad a_k u_k + b_k v_k = a \wedge b$$

Par définition de l'algorithme d'Euclide C12.30 :

$$(\star\star) \qquad a_k = b_{k-1}$$

et b_k est le reste de la division euclidienne de a_{k-1} par b_{k-1}. Ainsi il existe $q_{k-1} \in \mathbb{Z}$ tel que :

$$(\star\star\star) \qquad a_{k-1} = b_{k-1} q_{k-1} + b_k \,.$$

De $(\star)$, $(\star\star)$ et $(\star\star\star)$, nous déduisons :

$$a \wedge b = b_{k-1} u_k + \left(a_{k-1} - b_{k-1} q_{k-1}\right) v_k = a_{k-1} \cdot \underbrace{v_k}_{u_{k-1} \in \mathbb{Z}} + b_{k-1} \cdot \underbrace{\left(u_k - q_{k-1} v_k\right)}_{v_{k-1} \in \mathbb{Z}} .$$

Avec la récurrence finie descendante précédente, il vient :

$$\exists (u_0, v_0) \in \mathbb{Z}^2 \quad a \wedge b = a_0 u_0 + b_0 v_0 = a u_0 + b v_0 \,.$$

Méthode

Soit $(a, b) \in \mathbb{N}^2$ tel que $1 \leqslant b < a$. Une relation de Bézout liant a, b et $a \wedge b$ peut être effectivement obtenue, en exploitant les divisions euclidiennes calculées lors de l'exécution de l'algorithme d'Euclide C12.30. Pour cela, il suffit d'effectuer des substitutions successives dans les identités livrées par les divisions euclidiennes, en commençant par l'avant dernière pour remontrer à la première. Cf. Démonstration précédente et exemple suivant.

C12.40. Exemple Nous calculons une relation de Bézout pour 255 et 141, en exploitant l'algorithme d'Euclide exécuté en C12.31, grâce auquel nous avons calculé $245 \wedge 141 = 3$.

Étape	Division euclidienne de a_k par b_k	Valeur de a_k	Valeur de b_k
0		$a_0 = 255$	$b_0 = 141$
1	$\underbrace{255}_{a_0} = 1 \cdot \underbrace{141}_{b_0} + \underbrace{114}_{\text{reste n°1}}$	$a_1 = b_0 = 141$	$b_1 = \text{reste n°1} = 114$
2	$\underbrace{141}_{a_1} = 1 \cdot \underbrace{114}_{b_1} + \underbrace{27}_{\text{reste n°2}}$	$a_2 = b_1 = 114$	$b_2 = \text{reste n°2} = 27$
3	$\underbrace{114}_{a_2} = 4 \cdot \underbrace{27}_{b_2} + \underbrace{6}_{\text{reste n°3}}$	$a_3 = b_2 = 27$	$b_3 = \text{reste n°3} = 6$
4	$\underbrace{27}_{a_3} = 4 \cdot \underbrace{6}_{b_3} + \underbrace{3}_{\text{reste n°4}}$	$a_4 = b_3 = 6$	$\underbrace{b_4 = \text{reste n°4} = 3}_{\text{dernier reste non nul}}$
5	$\underbrace{6}_{a_4} = 2 \cdot \underbrace{3}_{b_4} + \underbrace{0}_{\text{reste n°5}}$	$a_5 = b_4 = 3$	$b_5 = \text{reste n°5} = 0$

(4) D'après l'étape 4 :

$$3 = \underbrace{27}_{a_3} - 4 \cdot \underbrace{6}_{b_3} \qquad \text{[identité 4]}\ .$$

(3) D'après l'étape 3 :

$$a_3 = b_2 = 27 \qquad \text{et} \qquad \underbrace{6}_{b_3} = \underbrace{114}_{a_2} - 4 \cdot \underbrace{27}_{b_2}\ .$$

Avec l'identité 4, il vient :

$$3 = \underbrace{27}_{b_2} - 4 \cdot \left(\underbrace{114}_{a_2} - 4 \cdot \underbrace{27}_{b_2} \right) = -4 \cdot \underbrace{114}_{a_2} + 17 \cdot \underbrace{27}_{b_2} \qquad \text{[identité 3]}\ .$$

(2) D'après l'étape 2 :

$$a_2 = b_1 = 114 \qquad \text{et} \qquad \underbrace{27}_{b_2} = \underbrace{141}_{a_1} - \underbrace{114}_{b_1}\ .$$

Avec l'identité 3, il vient :

$$3 = -4 \cdot \underbrace{114}_{b_1} + 17 \cdot \left(\underbrace{141}_{a_1} - \underbrace{114}_{b_1} \right) = 17 \cdot \underbrace{141}_{a_1} - 21 \cdot \underbrace{114}_{b_1} \qquad \text{[identité 2]}\ .$$

(1) D'après l'étape 1 :

$$a_1 = b_0 = 141 \qquad \text{et} \qquad \underbrace{114}_{b_1} = \underbrace{255}_{a_0} - \underbrace{141}_{b_0}\ .$$

Avec l'identité 2, il vient :

$$3 = 17 \cdot \underbrace{141}_{b_0} - 21 \cdot \left(\underbrace{255}_{a_0} - \underbrace{141}_{b_0} \right) = -21 \cdot \underbrace{255}_{a_0 = a} + 38 \cdot \underbrace{141}_{b_0 = b}\ .$$

C12.41. Exercice Construire une fonction Python **Bezout** d'arguments :

- **a** un entier naturel non nul ;
- **b** un entier naturel non nul ;

qui renvoie un couple **(u,v)** d'entiers relatifs tel que **a u** + **b v** = **a** $\wedge$ **b** .

C12.42. Définition (PPCM de deux entiers naturels non tous les deux nuls)

- Soit $(a,b) \in \mathbb{Z}^2$. Le Plus Petit Commum Multiple (PPCM) de a et b, noté $a \vee b$, est défini par :

$$a \vee b = \min\left(\{ k \cdot |a| \ : \ k \in \mathbb{N}^* \} \cap \{ \ell \cdot |b| \ : \ \ell \in \mathbb{N}^* \} \right)$$

  où le min est relatif à la relation d'ordre $\leqslant$ usuelle sur $\mathbb{N}$.
- En particulier, si $(a,b) \in \mathbb{N}^* \times \mathbb{N}^*$, $a \vee b$ est le plus petit multiple strictement positif de a et b pour la relation d'ordre $\leqslant$ usuelle sur $\mathbb{N}$.

C12.43. Théorème (lien fondamental entre PGCD et PPCM) Soit $(a,b) \in \mathbb{Z}^2$.

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

Démonstration

- Si $a = 0$ ou $b = 0$ alors l'assertion est claire.
- Supposons désormais $a \neq 0$ et $b \neq 0$. Puisque $a \wedge b = |a| \wedge |b|$ et $a \vee b = |a| \vee |b|$, nous renforçons l'hypothèse et supposons que $a \in \mathbb{N}^*$ et $b \in \mathbb{N}^*$.
- Comme $a \wedge b$ divise a et b, il existe $(\alpha, \beta) \in \mathbb{N}^* \times \mathbb{N}^*$ tel que $a = \alpha \cdot a \wedge b$ et $b = \beta \cdot a \wedge b$. Nous observons que :
$$\alpha \cdot \beta \cdot a \wedge b = \beta \cdot a = \alpha \cdot b$$
est un multiple commun à a et b.
- Soit m un multiple commun à a et b. Alors il existe $(k, \ell) \in \mathbb{N}^* \times \mathbb{N}^*$ tel que $m = k \cdot a$ et $m = \ell \cdot b$. Nous allons établir que $\alpha \cdot \beta \cdot a \wedge b \mid m$, ce qui impliquera que $\alpha \cdot \beta \cdot a \wedge b \leqslant m$.
- Considérons une relation de Bézout pour (a,b) :
$$au + bv = a \wedge b$$
où $(u,v) \in \mathbb{Z}^2$. En multipliant chaque membre de cette égalité par $k \cdot \ell$, il vient :
$$k \cdot \ell \cdot a \wedge b = k \cdot \ell \cdot a \cdot u + k \cdot \ell \cdot b \cdot v = m \cdot (\ell \cdot u + k \cdot v)$$
puis, comme $m = k \cdot a = k \cdot \alpha \cdot a \wedge b$:
$$k \cdot \ell \cdot a \wedge b = k \cdot \alpha \cdot a \wedge b \cdot (\ell \cdot u + k \cdot v)\ .$$
Comme $k \cdot a \wedge b \neq 0$ et $\mathbb{Z}$ est intègre :
$$\ell = \alpha \cdot (\ell \cdot u + k \cdot v)\ .$$
Finalement :
$$m = \ell \cdot b = \alpha \cdot (\ell \cdot u + k \cdot v) \cdot \beta \cdot a \wedge b = \underbrace{(\ell \cdot u + k \cdot v)}_{\in \mathbb{Z}} \cdot \alpha \cdot \beta \cdot a \wedge b\,.$$
- D'après l'étude précédente, $a \vee b = \alpha \cdot \beta \cdot a \wedge b$. Ainsi :
$$a \vee b \cdot a \wedge b = \alpha \cdot a \wedge b \cdot \beta \cdot a \wedge b = a \cdot b\,.$$

C12.44. Remarque Au cours de la précédente démonstration, nous avons établi que, pour tout $(a,b) \in \mathbb{N}^* \times \mathbb{N}^*$:

$$a \vee b = \min\left(\{ka\,:\,k \in \mathbb{N}^*\} \cap \{\ell b\,:\,\ell \in \mathbb{N}^*\}\right)$$

où le min est relatif à la relation d'ordre $\mid$ sur $\mathbb{N}$.

C12.45. Exemple D'après C12.31, $255 \wedge 141 = 3$. D'après C12.43, $255 \vee 141$ est le quotient de $245 \cdot 141$ par 3, soit $255 \vee 141 = 85 \times 141 = 11\,985$.

§ 4 Entiers premiers entre eux

C12.46. Définition (entiers premiers entre eux)
Deux entiers relatifs a et b sont dits premiers entre eux si $a \wedge b = 1$.

C12.47. Exercice Soit $n \in \mathbb{N}$. Démontrer que n et $n+1$ sont premiers entre eux.

- D'une part 1 divise n et $n+1$. Ainsi $\{1\} \subset \mathrm{Div}(n) \cap \mathrm{Div}(n+1)$.
- D'autre part, si $d \in \mathbb{N}^*$ divise n et $n+1$ alors il existe $(q_1, q_2) \in \mathbb{N}^2$ tel que $n = q_1 d$ et $n+1 = q_2 d$. Ainsi :

$$1 = n+1-n = \underbrace{(q_2 - q_1)}_{\in \mathbb{Z}} \cdot d \, .$$

Le nombre d est un diviseur positif de 1 donc $d = 1$. Ainsi $\mathrm{Div}(n) \cap \mathrm{Div}(n+1) \subset \{1\}$.

- D'après les deux points précédents, $\mathrm{Div}(n) \cap \mathrm{Div}(n+1) = \{1\}$ et donc :

$$n \wedge (n+1) = \max(\mathrm{Div}(n) \cap \mathrm{Div}(n+1)) = \max(\{1\}) = 1 \, .$$

C12.48. Théorème (de Bézout) Soit $(a, b) \in \mathbb{Z}^2$.

$$a \wedge b = 1 \iff \left(\exists (u, v) \in \mathbb{Z}^2 \quad au + bv = 1\right)$$

Démonstration

Nous ne considérons que le cas où a et b sont des entiers naturels non tous les deux nuls.

$\Longrightarrow$ Il s'agit d'une conséquence de l'existence d'une relation de Bézout (C12.39).

$\Longleftarrow$ Supposons qu'il existe $(u, v) \in \mathbb{Z}^2$ tel que $au + bv = 1$.

- D'une part 1 divise a et b. Ainsi $\{1\} \subset \mathrm{Div}(a) \cap \mathrm{Div}(b)$.
- D'autre part, si $d \in \mathbb{N}^*$ divise a et b alors il existe $(q_1, q_2) \in \mathbb{N}^2$ tel que $a = q_1 d$ et $b = q_2 d$. Ainsi :

$$1 = au + bv = \underbrace{(uq_1 + vq_2)}_{\in \mathbb{Z}} \cdot d \, .$$

Le nombre d est un diviseur positif de 1 donc $d = 1$. Ainsi $\mathrm{Div}(a) \cap \mathrm{Div}(b) \subset \{1\}$.

- D'après les deux points précédents, $\mathrm{Div}(a) \cap \mathrm{Div}(b) = \{1\}$ et donc :

$$a \wedge b = \max(\mathrm{Div}(a) \cap \mathrm{Div}(b)) = \max(\{1\}) = 1 \, .$$

C12.49. Forme irréductible d'un nombre rationnel

$$\forall r \in \mathbb{Q}^* \quad \exists (\alpha, \beta) \in \mathbb{Z} \times \mathbb{N}^* \quad r = \frac{\alpha}{\beta} \text{ et } \alpha \wedge \beta = 1$$

Démonstration

Soit $r \in \mathbb{Q}^*$. Alors il existe $(a,b) \in \mathbb{Z} \times \mathbb{N}^*$ tel que $r = \dfrac{a}{b}$. Considérons une relation de Bézout (C12.39) pour (a,b) :

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

où $(u,v) \in \mathbb{Z}^2$. Comme $a \wedge b \neq 0$ divise a et b, il existe $(\alpha,\beta) \in \mathbb{Z} \times \mathbb{N}^*$ tel que $a = \alpha \cdot a \wedge b$ et $b = \beta \cdot a \wedge b$, il vient :

$$a \wedge b = a \wedge b \cdot (\alpha u + \beta v) \quad \text{et} \quad r = \frac{a}{b} = \frac{\alpha \cdot a \wedge b}{\beta \cdot a \wedge b} = \frac{\alpha}{\beta}$$

Comme $\mathbb{Z}$ est intègre et $a \wedge b \neq 0$, il vient $1 = \alpha u + \beta v$. D'après le théorème de Bézout (C12.48), $\alpha \wedge \beta = 1$.

C12.50. Exercice Soit $(a,b) \in \mathbb{Z}^2$ tel que $a \wedge b = 1$. Alors, pour tout $(m,n) \in \mathbb{N}^* \times \mathbb{N}^*$, $a^m \wedge b^n = 1$.

Soit $(m,n) \in \mathbb{N}^* \times \mathbb{N}^*$. Considérons une relation de Bézout (C12.39) pour (a,b) :

$$au + bv = 1\,.$$

où $(u,v) \in \mathbb{Z}^2$. D'après la formule du binôme de Newton :

$$1^{m+n} = (au+bv)^{m+n} = \sum_{k=0}^{m-1} \binom{m+n}{k} \cdot a^k \cdot u^k \cdot b^{m+n-k} \cdot v^{m+n-k} + \sum_{k=m}^{m+n} \binom{m+n}{k} \cdot a^k \cdot u^k \cdot b^{m+n-k} \cdot v^{m+n-k}\,.$$

Comme :

$$\sum_{k=0}^{m-1} \binom{m+n}{k} \cdot a^k \cdot u^k \cdot b^{m+n-k} \cdot v^{m+n-k} = b^n \cdot \underbrace{\sum_{k=0}^{m-1} \binom{m+n}{k} \cdot a^k \cdot u^k \cdot b^{m-k} \cdot v^{m+n-k}}_{=:v' \in \mathbb{Z} \text{ car } m-k \geqslant 0 \text{ si } k \in [\![0, m-1]\!]}$$

et

$$\sum_{k=m}^{m+n} \binom{m+n}{k} \cdot a^k \cdot u^k \cdot b^{m+n-k} \cdot v^{m+n-k} = a^m \cdot \underbrace{\sum_{k=m}^{m+n} \binom{m+n}{k} \cdot a^{k-m} \cdot u^k \cdot b^{m+n-k} \cdot v^{m+n-k}}_{=:u' \in \mathbb{Z} \text{ car } k-m \geqslant 0 \text{ si } k \in [\![m, m+n]\!]}$$

il vient :

$$1 = b^n \cdot v' + a^m \cdot u'\,.$$

D'après le théorème de Bézout (C12.48), $a^m \wedge b^n = 1$.

Soit $(a,b) \in \mathbb{Z}^2$. S'il existe $(u,v,d) \in \mathbb{Z} \times \mathbb{Z} \times \mathbb{N}$ tel que $au + bv = d$, alors d n'est pas nécessairement le PGCD de a et b. En effet :

$$\underbrace{3}_{a} \cdot \underbrace{2}_{u} + \underbrace{2}_{b} \cdot \underbrace{(-2)}_{v} = \underbrace{2}_{d}$$

mais $3 \wedge 2 = 1$.

C12.51. Lemme (de Gauss) Soit $(a,b,c) \in \mathbb{N}^3$.

$$(a \mid bc \text{ et } a \wedge b = 1) \implies a \mid c$$

Démonstration

Supposons que $a \mid bc$ et que $a \wedge b = 1$. Alors il existe $(q,u,v) \in \mathbb{N} \times \mathbb{Z} \times \mathbb{Z}$ tel que :

$$bc = qa \qquad \text{et} \qquad 1 = au + bv\,.$$

En multipliant chaque membre de cette dernière identité par c, il vient :

$$c = acu + bcv = acu + qav = a \cdot \underbrace{(cu + qv)}_{\in \mathbb{Z}}$$

et donc a divise c.

C12.52. Corollaire Soit $(a,b,n) \in \mathbb{N}^3$.

$$(a \wedge n = 1 \text{ et } b \wedge n = 1) \implies (ab) \wedge n = 1$$

Démonstration

Supposons $a \wedge n = 1$ et $b \wedge n = 1$. Considérons des relations de Bézout (C12.39) pour (a,n) et (b,n) :

$$au_1 + nv_1 = 1 \qquad \text{et} \qquad bu_2 + nv_2 = 1$$

où $(u_1,v_1,u_2,v_2) \in \mathbb{Z}^4$. En multipliant membre-à-membre ces deux identités, nous obtenons :

$$1 = (au_1 + nv_1)(bu_2 + nv_2) = ab \cdot \underbrace{u_1u_2}_{\in \mathbb{Z}} + n \cdot \underbrace{(au_1v_2 + v_1bu_2 + v_1nv_2)}_{\in \mathbb{Z}}\,.$$

D'après le théorème de Bézout (C12.48), $(ab) \wedge n = 1$.

♥ Le théorème de Bézout est un outil puissant pour démontrer des primalités relatives. Il est d'une grande utilité, tout comme le lemme de Gauß.

§ 5 Nombres premiers

C12.53. Définition (nombre premier) Un nombre premier est un entier naturel p tel que :

- $p \geqslant 2$;
- les seuls diviseurs positifs de p sont 1 et p.

C12.54. Exemple Les nombres :

2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59 61 67 71 73 79 83 89 97

sont les nombres premiers appartenant à $[\![2,100]\!]$.

C12.55. Remarque Si $n \geqslant 4$ est un nombre entier non premier, alors :

$$\exists (a,b) \in [\![2, n-1]\!]^2 \quad n = ab\,.$$

En effet, comme $n \geqslant 2$ et n n'est pas premier, n possède un diviseur positif a distinct de 1 et n. Ainsi $a \in [\![2, n-1]\!]$. Notons b le quotient de la division de n par a, de sorte que $n = ab$. Comme $a > 1$, $b < n$ et comme $a < n$, $b > 1$. Ainsi $b \in [\![2, n-1]\!]$.

C12.56. Lemme Tout entier $n \geqslant 2$ possède un diviseur premier.

Démonstration

- Nous raisonnons par l'absurde et supposons qu'il existe $n \geqslant 2$ sans diviseur premier.
- Alors :

$$A := \{k \in \mathbb{N} : \ k \geqslant 2 \text{ et } k \text{ ne possède aucun diviseur premier}\}$$

est une partie non vide de $\mathbb{N}$. Comme $\mathbb{N}$ vérifie la propriété de bon ordre, A possède un plus petit élément que nous notons m.
- L'entier m n'est pas premier (sinon il n'appartiendrait pas à A puisque $m \mid m$). Donc $m \geqslant 4$ et d'après C12.55 il existe $(a,b) \in [\![2, m-1]\!]^2$ tel que $m = ab$.
- Puisque $2 \leqslant a < m$, $a \notin A$ et donc l'entier a possède un diviseur premier p. Comme $p \mid a$ et $a \mid m$, $p \mid m$ (transitivité de la relation d'ordre $\mid$ sur $\mathbb{N}$) d'où une contradiction.

C12.57. Proposition (crible d'Eratosthène) Soit un nombre entier $n \geqslant 2$.

Si aucun nombre premier $p \in [\![2, \lfloor \sqrt{n} \rfloor]\!]$ ne divise n alors n est premier.

Démonstration

- Nous raisonnons par contraposition. Supposons donc que n n'est pas premier et démontrons qu'alors n possède un diviseur premier p tel que $2 \leqslant p \leqslant \lfloor \sqrt{n} \rfloor$.
- Comme n n'est pas premier, $n \geqslant 4$ et d'après C12.55 il existe $(a,b) \in [\![2, n-1]\!]^2$ tel que $n = ab$.
- Si $a > \lfloor \sqrt{n} \rfloor$ et $b > \lfloor \sqrt{n} \rfloor$ alors, comme a et b sont entiers :

$$a \geqslant \lfloor \sqrt{n} \rfloor + 1 > \sqrt{n} \qquad \text{et} \qquad b \geqslant \lfloor \sqrt{n} \rfloor + 1 > \sqrt{n}$$

d'où $n = ab > n$, ce qui n'est pas. Ainsi $a \leqslant \lfloor \sqrt{n} \rfloor$ ou $b \leqslant \lfloor \sqrt{n} \rfloor$. Quitte à échanger les rôles joués par a et b, nous pouvons supposer $a \leqslant \lfloor \sqrt{n} \rfloor$.
- D'après C12.56, il existe un nombre premier p divisant a donc inférieur ou égal à a. Ainsi $p \leqslant a \leqslant \lfloor \sqrt{n} \rfloor$ et p divise n ($p \mid a$, $a \mid n$ et transitivité de la relation d'ordre $\mid$ sur $\mathbb{N}$).

C12.58. Exemple L'entier 151 est premier.
En effet, les nombres premiers plus petits que $\lfloor \sqrt{151} \rfloor = 12$ sont $2, 3, 5, 7, 11$. Or ces cinq nombres premiers ne divisent pas 151 puisque :

$$151 = 2 \cdot 75 + 1 \qquad 151 = 3 \cdot 50 + 1 \qquad 151 = 5 \cdot 30 + 1 \qquad 151 = 7 \cdot 21 + 4 \qquad 151 = 11 \cdot 13 + 8\,.$$

D'après le crible d'Eratosthène (C12.57), 151 est premier.

C12.59. Remarque Deux nombres premiers distincts p_1 et p_2 sont premiers entre eux.
En effet $\mathrm{Div}(p_1) \cap \mathrm{Div}(p_2) = \{1, p_1\} \cap \{1, p_2\} = \{1\}$ et donc $p_1 \wedge p_2 = \max(\mathrm{Div}(p_1) \cap \mathrm{Div}(p_2)) = \max(\{1\}) = 1$.

C12.60. Exercice Construire une fonction Python **estPremier** d'argument un entier **n** qui renvoie **True** si **n** est premier et **False** sinon, en s'appuyant sur le crible d'Eratosthène.

C12.61. Proposition (l'ensemble des nombres premiers est infini) L'ensemble

$$\mathscr{P} := \{n \in \mathbb{N} : n \text{ est premier}\}$$

des nombres premiers est infini.

Démonstration

- Raisonnons par l'absurde et supposons $\mathscr{P}$ fini. Nous pouvons alors considérer une liste finie, exhaustive et sans répétition des nombres premiers : $p_1, p_2, \dots, p_r$.
- L'entier $n := 1 + \prod_{i=1}^{r} p_i$ est supérieur ou égal à 2. Il possède donc un diviseur premier (C12.56) qui est nécessairement l'un des premiers $p_1, p_2, \dots, p_r$.
- Nous obtenons une contradiction, puisqu'aucun des entiers $p_1, p_2, \dots, p_r$ ne divise n. En effet le reste de la division euclidienne de n par p_i ($i \in [\![1, r]\!]$) est 1.

C12.62. Remarque (répartition des nombres premiers) La répartition des nombres premiers parmi les entiers est *a priori* irrégulière. Citons toutefois deux résultats, dont les démonstrations connues dépassent le cadre du programme de MP2I, qui nous apportent quelques informations sur celle-ci.

1. *Postulat de Bertrand.*

   Pour tout entier $n \geqslant 2$, il existe un nombre premier appartenant à $[\![n+1, 2n-1]\!]$.

   Il fut énoncé par Joseph Bertrand en 1845 et démontré par Pafnouti Tchebychev en 1850.

2. *Théorème des nombres premiers.* Si, pour tout entier $n \geqslant 2$, on note $\pi(n)$ le nombre de premiers appartenant à $[\![2, n]\!]$, alors :

   $$\pi(n) \sim \frac{n}{\ln(n)}.$$

   Il fut démontré indépendamment par Jacques Hadamard et Charles de la Vallée Poussin en 1896. On pourra lire avec intérêt l'article de Michèle Audin à ce sujet **[Lien]**.

C12.63. Lemme (pierre angulaire) Soient :

- p un nombre premier et $\alpha \in \mathbb{N}^*$;
- $s \in \mathbb{N}^*$, $q_1, \dots, q_s$ des premiers deux-à-deux distincts et $\beta_1, \dots, \beta_s$ des entiers naturels non nuls.

On suppose que p^α divise $\prod_{\ell=1}^{s} q_\ell^{\beta_\ell}$.

$$\exists! i \in [\![1, s]\!] \quad p = q_i \text{ et } \alpha \leqslant \beta_i .$$

Démonstration

(1) Démontrons que $p \in \{q_1, \dots, q_s\}$ en raisonnant par l'absurde. Supposons donc que $p \notin \{q_1, \dots, q_s\}$.
D'après cette hypothèse, p est premier avec $q_1, \dots, q_s$ (C12.59) donc premier avec $q_1^{\beta_1}, \dots, q_s^{\beta_s}$ (C12.50). D'après C12.52, p est premier avec $\prod_{\ell=1}^{s} q_\ell^{\beta_\ell}$, ce qui n'est pas puisque p divise $\prod_{\ell=1}^{s} q_\ell^{\beta_\ell}$ $(\alpha \geqslant 1)$.
(2) Comme $p \in \{q_1, \dots, q_s\}$ et $q_1, \dots, q_s$ sont deux-à-deux distincts, il existe un unique $i \in [\![1, s]\!]$ tel que $p = q_i$.
(3) Démontrons que $\alpha \leqslant \beta_i$ en raisonnant par l'absurde. Supposons donc $\alpha > \beta_i$.
Puisque p^α divise $\prod_{\ell=1}^{s} q_\ell^{\beta_\ell}$ il existe un entier a tel que $\prod_{\ell=1}^{s} q_\ell^{\beta_\ell} = a \cdot p^\alpha$.
Nous en déduisons $\prod_{\substack{\ell=1 \\ \ell \neq i}}^{s} q_\ell^{\beta_\ell} = a \cdot p^{\alpha-\beta_i}$ et donc $p^{\alpha-\beta_i}$ divise $\prod_{\substack{\ell=1 \\ \ell \neq i}}^{s} q_\ell^{\beta_\ell}$ avec $\alpha - \beta_i \in \mathbb{N}^*$.
D'après **(1)**, $p = q_i$ appartient à $\{q_\ell : \ell \in [\![1, s]\!] \setminus \{i\}\}$, ce qui contredit le caractère deux-à-deux distinct de $q_1, \dots, q_s$.

C12.64. Théorème (fondamental de l'arithmétique) Soit un nombre entier $n \geqslant 2$.

(1) Existence Il existe :

- $r \in \mathbb{N}^*$;
- un r-uplet de nombres premiers $(p_1, \dots, p_r)$ deux-à-deux distincts ;
- un r-uplet d'entiers naturels non nuls $(\alpha_1, \dots, \alpha_r)$

tels que $n = \prod_{k=1}^{r} p_k^{\alpha_k}$.

(2) Unicité à l'ordre des facteurs près Soient :

- $r \in \mathbb{N}^*$ et $s \in \mathbb{N}^*$;
- un r-uplet de nombres premiers $(p_1, \dots, p_r)$ deux-à-deux distincts et un s-uplet de nombres premiers $(q_1, \dots, q_s)$ deux-à-deux distincts ;
- un r-uplet d'entiers naturels non nuls $(\alpha_1, \dots, \alpha_r)$ et un s-uplet d'entiers naturels non nuls $(\beta_1, \dots, \beta_s)$;

tels que $\prod_{k=1}^{r} p_k^{\alpha_k} = n = \prod_{\ell=1}^{s} q_\ell^{\beta_\ell}$. Alors :

(a) $r = s$;

(b) il existe une bijection $\varphi : [\![1, r]\!] \longrightarrow [\![1, s]\!]$ tel que, pour tout $k \in [\![1, r]\!]$:

$$p_k = q_{\varphi(k)} \quad \text{et} \quad \alpha_k = \beta_{\varphi(k)}.$$

C12.65. Remarque La bijection φ dans l'énoncé du théorème fondamental de l'arithmétique (C12.64) permet de formaliser l'unicité de la décomposition à l'ordre des facteurs près. Précisément, elle encode la permutation des facteurs.

Démonstration

(1) Nous démontrons l'existence d'une décomposition d'un entier naturel $n \geqslant 2$ en produit de nombres premiers, en raisonnant par récurrence forte.

Initialisation à $n = 2$ Si nous posons $r = 1$, $p_1 = 2 \in \mathscr{P}$ et $\alpha_1 = 1$, alors $2 = \prod_{k=1}^{r} p_k^{\alpha_k}$.

Hérédité Soit un entier $n \geqslant 2$ tel que tous les entiers $k \in [\![2, n]\!]$ possèdent une décomposition en produit de nombres premiers. Démontrons que $n+1$ possède lui aussi une décomposition en produit de nombres premiers.

(i) *Cas où $n+1$ est premier* Si nous posons $r = 1$, $p_1 = n+1 \in \mathscr{P}$ et $\alpha_1 = 1$, alors $n+1 = \prod_{k=1}^{r} p_k^{\alpha_k}$.

(ii) *Cas où $n+1$ n'est pas premier* D'après C12.56, il existe un nombre premier p qui divise $n+1$. Comme $n+1$ n'est pas premier, $p \neq n+1$ et donc $2 \leqslant p \leqslant n$. Notons $q \in \mathbb{N}^*$ tel que $n+1 = pq$. Comme $2 \leqslant p \leqslant n$, $2 \leqslant q \leqslant n$. D'après l'hypothèse de récurrence, il existe $r \in \mathbb{N}^*$, un r-uplet de nombres premiers $(p_1, \dots, p_r)$ deux-à-deux distincts, un r-uplet d'entiers naturels non nuls $(\alpha_1, \dots, \alpha_r)$ tels que :

$$q = \prod_{k=1}^{r} p_k^{\alpha_k}.$$

et donc $n+1 = pq = p \cdot \left(\prod_{k=1}^{r} p_k^{\alpha_k} \right)$.

(α) Si p est l'un des premiers $p_1, \dots, p_r$ alors il existe un unique $i \in [\![1, r]\!]$ tel que $p = p_i$. Si on pose, pour tout $k \in [\![1, r]\!]$:

$$\alpha'_k = \begin{cases} \alpha_i + 1 \in \mathbb{N}^* & \text{si } k = i ; \\ \alpha_k \in \mathbb{N}^* & \text{sinon} ; \end{cases}$$

il vient $n+1 = \prod_{k=1}^{r} p_k^{\alpha'_k}$ qui est une décomposition de la forme voulue.

(β) Si p n'est pas l'un des $p_1, \dots, p_r$ alors on pose :

$$p_{r+1} = p \qquad \text{et} \qquad \alpha_{r+1} = 1$$

de sorte que $n+1 = \prod_{k=1}^{r+1} p_k^{\alpha_k}$ qui est une décomposition de la forme voulue, en particulier les premiers $p_1, \dots, p_r, p_{r+1}$ sont deux-à-deux distincts.

(2) Passons à la démonstration de l'unicité. Soient un entier $n \geqslant 2$, deux entiers $(r, s) \in \mathbb{N}^* \times \mathbb{N}^*$, un r-uplet de nombres premiers $(p_1, \dots, p_r)$ deux-à-deux distincts, un s-uplet de nombres premiers $(q_1, \dots, q_s)$ deux-à-deux distincts, un r-uplet d'entiers naturels non nuls $(\alpha_1, \dots, \alpha_r)$ un s-uplet d'entiers naturels non nuls $(\beta_1, \dots, \beta_s)$ tels que :

$$(\star) \quad \prod_{k=1}^{r} p_k^{\alpha_k} = n = \prod_{\ell=1}^{s} q_\ell^{\beta_\ell}.$$

D'après le lemme C12.63 :

$$\forall\, k \in [\![1, r]\!] \quad \exists ! \varphi(k) \in [\![1, s]\!] \quad p_k = q_{\varphi(k)} \text{ et } \alpha_k \leqslant \beta_{\varphi(k)}.$$

et

$$\forall\, \ell \in [\![1, s]\!] \quad \exists ! \psi(\ell) \in [\![1, r]\!] \quad q_\ell = p_{\psi(\ell)} \text{ et } \beta_\ell \leqslant \alpha_{\psi(\ell)}.$$

Ainsi les applications :

$$\varphi \left| \begin{array}{ccc} [\![1,r]\!] & \longrightarrow & [\![1,s]\!] \\ k & \longmapsto & \varphi(k) \end{array} \right. \quad \text{et} \quad \psi \left| \begin{array}{ccc} [\![1,s]\!] & \longrightarrow & [\![1,r]\!] \\ \ell & \longmapsto & \psi(\ell) \end{array} \right.$$

sont bien définies. Comme les premiers $p_1, \dots, p_r$ sont deux-à-deux distincts et les premiers $q_1, \dots, q_s$ sont deux-à-deux distincts, nous obtenons :

$$\varphi \circ \psi = \mathrm{id}_{[\![1,s]\!]} \quad \text{et} \quad \psi \circ \varphi = \mathrm{id}_{[\![1,r]\!]}$$

Nous en déduisons que :

- $\varphi : [\![1,r]\!] \longrightarrow [\![1,s]\!]$ est bijective (d'application réciproque ψ) ;
- $r = s$;
- pour tout $k \in [\![1,r]\!]$, $p_k = q_{\varphi(k)}$ et puisque :

$$\alpha_k \leqslant \beta_{\varphi(k)} \quad \text{et} \quad \beta_{\varphi(k)} \leqslant \alpha_{\psi(\varphi(k))} = \alpha_k$$

$\alpha_k = \beta_{\varphi(k)}$.

C12.66. Exemple La décomposition de 12 345 678 en produit de nombres premiers est

$$12\,345\,678 = 2 \cdot 3^2 \cdot 47 \cdot 14\,593 .$$

C12.67. Exercice Construire une fonction Python **tfa** d'argument **n** un entier supérieur ou égal à 2 qui renvoie la liste des diviseurs premiers de **n** avec leurs exposants dans la décomposition de **n** en produit de facteurs premiers. Par exemple **tfa(123456)** renvoie **[(2,6),(3,1),(643,1)]** car $123\,456 = 2^6 \cdot 3^1 \cdot 643^1$.

C12.68. Définition (valuation p-adique d'un entier) Soient $n \in \mathbb{N}^*$ et p un nombre premier. La valuation p-adique de n est l'entier naturel $v_p(n)$ défini par :

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

C12.69. Exemple Comme $2^4 \mid 80$ et $2^5 \nmid 80$, $v_2(80) = 4$.

C12.70. Exercice Construire une fonction Python **valuation** d'arguments :

- **p** un nombre premier ;
- **n** un entier naturel non nul ;

qui renvoie la valuation **p**-adique de **n**.

C12.71. Caractérisation de la valuation p-adique d'un entier Soient $n \in \mathbb{N}^*$, p un nombre premier et $k \in \mathbb{N}$. D'après la définition de la valuation p-adique de n :

$$v_p(n) = k \text{ si et seulement s'il existe } a \in \mathbb{N}^* \text{ tel que } n = p^k a \text{ et } p \nmid a.$$

C12.72. Proposition (valuation p-adique et décomposition en produit de premiers)

Soit un entier $n \geqslant 2$. Considérons sa décomposition en produit de facteurs premiers $n = \prod_{k=1}^{r} p_k^{\alpha_k}$ où :

- $r \in \mathbb{N}^*$;
- $(p_1, \dots, p_r)$ est un r-uplet de premiers deux-à-deux distincts ;
- $(\alpha_1, \dots, \alpha_r)$ est un r-uplet d'entiers naturels non nuls.

Pour tout premier p :

$$v_p(n) = \begin{cases} \alpha_i & \text{s'il existe } i \in [\![1, r]\!] \text{ (nécessairement unique) tel que } p = p_i \\ 0 & \text{sinon.} \end{cases}$$

Démonstration

- Soit p un premier distinct de $p_1, \dots, p_r$. Alors $1 = p^0$ divise n et, d'après le lemme C12.63, $p = p^1$ ne divise pas n. Ainsi $v_p(n) = 0$.
- Soit $i \in [\![1, r]\!]$. Alors $p_i^{\alpha_i}$ divise n. Nous démontrons que $p_i^{\alpha_i+1}$ ne divise pas n, afin de conclure à $v_{p_i}(n) = \alpha_i$. Raisonnons par l'absurde et supposons que $p_i^{\alpha_i+1}$ divise n. Alors il existe $a \in \mathbb{N}^*$ tel que :

$$p_i^{\alpha_i+1} \cdot a = n = \prod_{k=1}^{r} p_k^{\alpha_k}.$$

Nous en déduisons que $p_i \cdot a = \prod_{\substack{k=1 \\ k \neq i}}^{r} p_k^{\alpha_k}$ et donc p_i divise $\prod_{\substack{k=1 \\ k \neq i}}^{r} p_k^{\alpha_k}$. D'après le lemme C12.63, $p_i \in \{p_k \,:\, k \in [\![1, r]\!] \setminus \{i\}\}$, ce qui n'est pas.

C12.73. Remarque Soit un entier $n \geqslant 2$. D'après C12.72, la décomposition de n en produit de facteurs premiers s'écrit :

$$n = \prod_{p \in \mathscr{P} \cap \mathrm{Div}(n)} p^{v_p(n)}.$$

Soit A une partie finie de $\mathbb{N}$ contenant $\mathrm{Div}(n)$. Comme pour tout $p \in \mathscr{P} \cap (A \setminus \mathrm{Div}(n))$, $v_p(n) = 0$ (p ne divise pas n) :

$$\prod_{p \in \mathscr{P} \cap A} p^{v_p(n)} = \left(\prod_{p \in \mathscr{P} \cap \mathrm{Div}(n)} p^{v_p(n)} \right) \cdot \underbrace{\left(\prod_{p \in \mathscr{P} \cap (A \setminus \mathrm{Div}(n))} p^{v_p(n)} \right)}_{=1} = \prod_{p \in \mathscr{P} \cap \mathrm{Div}(n)} p^{v_p(n)} = n.$$

C12.74. Proposition (valuations p-adiques d'un produit) Soient $(a, b) \in \mathbb{N}^* \times \mathbb{N}^*$ et $p \in \mathscr{P}$.

$$v_p(ab) = v_p(a) + v_p(b)$$

Démonstration

- Si $a = 1$ ou $b = 1$ alors l'assertion est triviale puisque $v_p(1) = 0$.
- Supposons désormais que $a \geqslant 2$ et $b \geqslant 2$. Comme $\mathrm{Div}(a) \cup \mathrm{Div}(b)$ est une partie finie de $\mathbb{N}$ contenant $\mathrm{Div}(a)$ et $\mathrm{Div}(b)$, nous savons (C12.73) :

$$a = \prod_{q \in \mathscr{P} \cap (\mathrm{Div}(a) \cup \mathrm{Div}(b))} q^{v_q(a)} \quad \text{et} \quad b = \prod_{q \in \mathscr{P} \cap (\mathrm{Div}(a) \cup \mathrm{Div}(b))} q^{v_q(b)}$$

d'où :

$$(\star) \qquad ab = \prod_{q \in \mathscr{P} \cap (\mathrm{Div}(a) \cup \mathrm{Div}(b))} q^{v_q(a)+v_q(b)}.$$

Comme, pour tout $q \in \mathscr{P} \cap (\mathrm{Div}(a) \cup \mathrm{Div}(b))$, q divise a ou b, $v_q(a) + v_q(b) \geqslant 1$. L'identité $(\star)$ est donc la décomposition de ab en produit de facteurs premiers (cf. C12.73). De $(\star)$ et C12.73, nous déduisons :

$$v_p(ab) = \begin{cases} v_p(a) + v_p(b) & \text{si } p \in \mathrm{Div}(a) \cup \mathrm{Div}(b) \\ 0 = \underbrace{v_p(a)}_{=0} + \underbrace{v_p(b)}_{=0} & \text{si } p \notin \mathrm{Div}(a) \cup \mathrm{Div}(b). \end{cases}$$

C12.75. Proposition (divisibilité via les valuations p-adiques) Soit $(a, b) \in \mathbb{N}^* \times \mathbb{N}^*$.

$$a \mid b \iff \left(\forall\, p \in \mathscr{P} \quad v_p(a) \leqslant v_p(b)\right)$$

Démonstration

$\Longrightarrow$ Supposons que a divise b. Alors il existe $c \in \mathbb{N}^*$ tel que $b = ac$. D'après C12.74, pour tout $p \in \mathscr{P}$:

$$v_p(b) = v_p(a) + \underbrace{v_p(c)}_{\geqslant 0} \geqslant v_p(a).$$

$\Longleftarrow$ Supposons que, pour tout $p \in \mathscr{P}$, $v_p(a) \leqslant v_p(b)$. D'après C12.73 :

$$\begin{aligned} b &= \prod_{p \in \mathscr{P} \cap (\mathrm{Div}(a) \cup \mathrm{Div}(b))} p^{v_p(b)} \\ &= \underbrace{\left(\prod_{p \in \mathscr{P} \cap (\mathrm{Div}(a) \cup \mathrm{Div}(b))} p^{v_p(a)} \right)}_{a} \cdot \underbrace{\left(\prod_{p \in \mathscr{P} \cap (\mathrm{Div}(a) \cup \mathrm{Div}(b))} p^{v_p(b)-v_p(a)} \right)}_{=:c} \end{aligned}$$

Comme, pour tout $p \in \mathscr{P} \cap (\mathrm{Div}(a) \cup \mathrm{Div}(b))$, $v_p(b) - v_p(a) \geqslant 0$, $c \in \mathbb{N}^*$ et donc a divise b.

C12.76. Proposition (PGCD et PPCM via les valuations p-adiques) Soit $(a, b) \in \mathbb{N}^* \times \mathbb{N}^*$.

$$a \wedge b = \prod_{p \in \mathscr{P} \cap (\mathrm{Div}(a) \cup \mathrm{Div}(b))} p^{\min\{v_p(a), v_p(b)\}} \quad \text{et} \quad a \vee b = \prod_{p \in \mathscr{P} \cap (\mathrm{Div}(a) \cup \mathrm{Div}(b))} p^{\max\{v_p(a), v_p(b)\}}$$

Nous démontrons uniquement le résultat pour le PGCD, le résultat pour le PPCM pouvant être établi de manière analogue. Précisément, nous établissons que :

$$d := \prod_{p \in \mathscr{P} \cap (\mathrm{Div}(a) \cup \mathrm{Div}(b))} p^{\min\{v_p(a), v_p(b)\}}$$

est le plus grand commun diviseur de a et b pour la relation d'ordre $\mid$ sur $\mathbb{N}$.

Démonstration

- Commençons par établir que :

$$\forall\, p \in \mathscr{P} \quad v_p(d) = \min\{v_p(a), v_p(b)\}\ .$$

Soit $p \in \mathscr{P}$.

— Si $p \in \mathrm{Div}(a) \cup \mathrm{Div}(b)$, alors $v_p(d) = \min\{v_p(a), v_p(b)\}$ découle de la définition de d et de C12.73.

— Si $p \notin \mathrm{Div}(a) \cup \mathrm{Div}(b)$, alors d'après C12.73 :

$$v_p(d) = 0 = v_p(a) = v_p(b)$$

et donc $v_p(d) = \min\{v_p(a), v_p(b)\}$.

- Démontrons ensuite que d divise a et b. Comme, pour tout $p \in \mathscr{P}$:

$$v_p(d) = \min\{v_p(a), v_p(b)\} \leqslant v_p(a) \qquad \text{et} \qquad v_p(d) = \min\{v_p(a), v_p(b)\} \leqslant v_p(b)$$

nous déduisons de C12.75 que d divise a et b.

- Soit $d' \in \mathbb{N}^*$ un diviseur commun à a et b. D'après C12.75, pour tout $p \in \mathscr{P}$:

$$v_p(d') \leqslant v_p(a) \qquad \text{et} \qquad v_p(d') \leqslant v_p(b)$$

donc, pour tout $p \in \mathscr{P}$:

$$v_p(d') \leqslant \min\{v_p(a), v_p(b)\} = v_p(d)\ .$$

D'après C12.75, d' divise d.

C12.77. Remarque La proposition C12.76 permet de fournir une nouvelle démonstration de la relation fondamentale liant le PGCD et le PPCM C12.43. En effet, si $(a, b) \in \mathbb{N}^* \times \mathbb{N}^*$:

$$\begin{aligned}
a \wedge b \cdot a \vee b &= \left(\prod_{p \in \mathscr{P} \cap (\mathrm{Div}(a) \cup \mathrm{Div}(b))} p^{\min\{v_p(a), v_p(b)\}}\right) \cdot \left(\prod_{p \in \mathscr{P} \cap (\mathrm{Div}(a) \cup \mathrm{Div}(b))} p^{\max\{v_p(a), v_p(b)\}}\right) \\
&= \prod_{p \in \mathscr{P} \cap (\mathrm{Div}(a) \cup \mathrm{Div}(b))} p^{\min\{v_p(a), v_p(b)\} + \max\{v_p(a), v_p(b)\}} \\
&= \prod_{p \in \mathscr{P} \cap (\mathrm{Div}(a) \cup \mathrm{Div}(b))} p^{v_p(a) + v_p(b)} \\
&= \left(\prod_{p \in \mathscr{P} \cap (\mathrm{Div}(a) \cup \mathrm{Div}(b))} p^{v_p(a)}\right) \cdot \left(\prod_{p \in \mathscr{P} \cap (\mathrm{Div}(a) \cup \mathrm{Div}(b))} p^{v_p(b)}\right) \\
&= a \cdot b \qquad [\text{C12.73}]\ .
\end{aligned}$$

§ 6 Congruences

C12.78. Notation Dans toute cette partie, n désigne un nombre entier naturel non nul.

C12.79. Définition Soit $(a,b) \in \mathbb{Z}^2$. On dit que a et b sont congrus modulo n et on note $a \equiv b\,[n]$ si

$$n \mid a-b.$$

C12.80. Exemple $123 \equiv 200\,[7]$ car 7 divise $200-123=77$.

C12.81. Proposition (caractérisation de la congruence par les restes) Soit $(a,b) \in \mathbb{Z}^2$.

$$a \equiv b\,[n] \iff a \text{ et } b \text{ ont même reste dans la division euclidienne par } n$$

Démonstration

$\Longrightarrow$ Supposons que $a \equiv b\,[n]$ alors il existe $q \in \mathbb{Z}$ tel que :

$$(\star) \quad a-b = qn\,.$$

Considérons la division euclidienne de a par n :

$$(\star\star) \quad a = q_a n + r_a$$

où $q_a \in \mathbb{Z}$ et $r_a \in [\![0, n-1]\!]$. De $(\star)$ et $(\star\star)$ on déduit :

$$b = \underbrace{(q_a - q)}_{\in\mathbb{Z}} \cdot n + r_a$$

et donc r_a est le reste de la division euclidienne de b par n.

$\Longleftarrow$ Considérons les divisions euclidiennes de a par n et de b par n :

$$a = q_a n + r_a \qquad \text{et} \qquad b = q_b n + r_b$$

où $(q_a, q_b) \in \mathbb{Z}^2$ et $(r_a, r_b) \in [\![0, n-1]\!]^2$. Supposons que $r_a = r_b$. Alors :

$$a - b = \underbrace{(q_a - q_b)}_{\in\mathbb{Z}} \cdot n$$

et donc $a \equiv b\,[n]$.

C12.82. Proposition La relation de congruence modulo n est une relation d'équivalence sur $\mathbb{Z}$, i.e. :

- $\forall\, a \in \mathbb{Z} \quad a \equiv a\,[n]$ [réflexivité]
- $\forall\, (a,b) \in \mathbb{Z}^2 \quad a \equiv b\,[n] \implies b \equiv a\,[n]$ [symétrie]
- $\forall\, (a,b,c) \in \mathbb{Z}^3 \quad (a \equiv b\,[n] \text{ et } b \equiv c\,[n]) \implies a \equiv c\,[n]$ [transitivité]

Démonstration

Les trois propriétés (réflexivité, symétrie et transitivité) s'établissent aisément en utilisant la caractérisation de la relation de congruence par les restes (C12.81).

C12.83. Proposition (classes d'équivalence modulo n) La relation de congruence possède n classes d'équivalence, données par les :

$$\overline{r} = \{r + kn \,:\, k \in \mathbb{Z}\}$$

où $r \in [\![0, n-1]\!]$.

Démonstration

- Soit $a \in \mathbb{Z}$. Si l'on note r le reste de la division euclidienne de a par n, alors d'après la caractérisation de la relation de congruence par les restes (C12.81), $a \equiv r\ [n]$ et donc $\overline{a} = \overline{r}$. Ainsi la liste :
$$\left\{\overline{r} \,:\, r \in [\![0, n-1]\!]\right\}$$
est une liste exhaustive des classes d'équivalence modulo n.
- D'après la caractérisation de la relation de congruence par les restes (C12.81), si $(r_1, r_2) \in [\![0, n-1]\!]^2$ alors $r_1 \not\equiv r_2\ [n]$ et donc $\overline{r_1} \neq \overline{r_2}$. Ainsi la liste :
$$\left\{\overline{r} \,:\, r \in [\![0, n-1]\!]\right\}$$
est une liste exhaustive et sans répétition des classes d'équivalence modulo n.
- Soit $r \in [\![0, n-1]\!]$.
  - Si $a \in \overline{r}$ alors $a \equiv r\ [n]$ et donc $a - r$ est divisible par n. Ainsi il existe $q \in \mathbb{Z}$ tel que $a - r = qn$ et par suite $a \in \{r + kn \,:\, k \in \mathbb{Z}\}$.
  - Si $a \in \{r + kn \,:\, k \in \mathbb{Z}\}$ alors il existe $k \in \mathbb{Z}$ tel que $a = r + kn$ et donc n divise $a - r$. Nous en déduisons $a \equiv r\ [n]$ et donc $a \in \overline{r}$.

D'après les deux inclusions précédentes, $\overline{r} = \{r + kn \,:\, k \in \mathbb{Z}\}$.

C12.84. Proposition (compatibilité de la relation de congruence avec les opérations)

1. La relation de congruence modulo n est compatible avec l'addition :
$$\forall (a,b,c,d) \in \mathbb{Z}^2 \quad (a \equiv b\ [n] \text{ et } c \equiv d\ [n]) \implies a + c \equiv b + d\ [n]$$
2. La relation de congruence modulo n est compatible avec la multiplication :
$$\forall (a,b,c,d) \in \mathbb{Z}^2 \quad (a \equiv b\ [n] \text{ et } c \equiv d\ [n]) \implies ac \equiv bd\ [n]$$
3. La relation de congruence modulo n est compatible avec les puissances :
$$\forall (a,b,k) \in \mathbb{Z} \times \mathbb{Z} \times \mathbb{N} \quad a \equiv b\ [n] \implies a^k \equiv b^k\ [n]$$

Démonstration

(1),(2) Soient $(a,b,c,d) \in \mathbb{Z}^2$ tel que $a \equiv b\ [n]$ et $c \equiv d\ [n]$. Alors il existe $q_1 \in \mathbb{Z}$ et $q_2 \in \mathbb{Z}$ tels que $a = b + q_1 n$ et $c = d + q_2 n$. Comme :

$$a + c = b + d + \underbrace{(q_1 + q_2)}_{\in\mathbb{Z}} \cdot n \quad \text{et} \quad ac = bd + \underbrace{(bq_2 + q_1 d + q_1 q_2 n)}_{\in\mathbb{Z}} \cdot n$$

on a $a + c \equiv b + d\ [n]$ et $ac \equiv bd\ [n]$.
(3) se déduit de **(2)** à l'aide d'un raisonnement par récurrence sur $k \in \mathbb{N}$ laissé en exercice.

C12.85. Exercice Soit $N \in \mathbb{N}^*$ d'écriture en base 10 notée $N = \sum_{k=0}^{p} a_k 10^k$, où $p \in \mathbb{N}$ et $(a_0, \dots, a_p) \in [\![0,9]\!]^{p+1}$ avec $a_p \neq 0$. Démontrer que 9 divise N si et seulement si 9 divise $\sum_{k=0}^{p} a_k$.

Il suffit de démontrer que $N \equiv \sum_{k=0}^{p} a_k \ [9]$ pour établir l'assertion. De $10 \equiv 1 \ [9]$ et de la compabilité de la relation de congruence avec les opérations (C12.84), nous déduisons :

$$\begin{aligned} N &\equiv \sum_{k=0}^{p} a_k 10^k \quad [9] \\ &\equiv \sum_{k=0}^{p} a_k \cdot 1^k \quad [9] \\ &\equiv \sum_{k=0}^{p} a_k \quad [9] \end{aligned}$$

C12.86. Proposition (inversibilité et inverse modulo n) Soit $a \in \mathbb{Z}$.

$$(\exists b \in \mathbb{Z} \quad ab \equiv 1 \ [n]) \iff a \wedge n = 1$$

Démonstration

$\Longrightarrow$ Supposons qu'il existe $b \in \mathbb{Z}$ tel que $ab \equiv 1 \ [n]$. Nous savons qu'alors il existe $q \in \mathbb{Z}$ tel que $ab - 1 = qn$, d'où :

$$a \cdot b + n \cdot (-q) = 1 \, .$$

D'après le théorème de Bézout (C12.48), $a \wedge n = 1$.

$\Longleftarrow$ Supposons que $a \wedge n = 1$ et considérons une relation de Bézout pour (a, n) (C12.39) :

$$au + nv = 1$$

où $(u, v) \in \mathbb{Z}^2$. Nous en déduisons que $au \equiv 1 \ [n]$ et donc $b = u$ convient.

Méthode

D'après la démonstration précédente, si $a \in \mathbb{Z}$ est premier avec n alors on peut déterminer un entier relatif b tel que $ab \equiv 1 \ [n]$ en calculant une relation de Bézout pour (a, n). Nous rappelons qu'une telle peut s'obtenir en « remontant » l'algorithme d'Euclide.

C12.87. Exercice Résoudre l'équation :

$$(E) \qquad 124 \cdot x + 5 = 16 \ [453]$$

d'inconnue $x \in \mathbb{Z}$.

- Calculons le PGCD de 453 et 124 avec l'algorithme d'Euclide.

$$\begin{aligned} 453 &= 3\cdot 124 + 81 \\ 124 &= 1\cdot 81 + 43 \\ 81 &= 1\cdot 43 + 38 \\ 43 &= 1\cdot 38 + 5 \\ 38 &= 7\cdot 5 + 3 \\ 5 &= 1\cdot 3 + 2 \\ 3 &= 1\cdot 2 + 1 \\ 2 &= 2\cdot 1 + 0 \end{aligned}$$

Donc $124 \wedge 453 = 1$.

- Déterminons alors une relation de Bézout pour $(124, 453)$ en « remontant » l'algorithme d'Euclide.

$$\begin{aligned} 1 &= 3-2 \\ &= 3-(5-3) = 2\cdot 3 - 5 \\ &= 2\cdot(38-7\cdot 5) - 5 = 2\cdot 38 - 15\cdot 5 \\ &= 2\cdot 38 - 15\cdot(43-38) = -15\cdot 43 + 17\cdot 38 \\ &= -15\cdot 43 + 17\cdot(81-43) = -32\cdot 43 + 17\cdot 81 \\ &= -32\cdot(124-81) + 17\cdot 81 = -32\cdot 124 + 49\cdot 81 \\ &= -32\cdot 124 + 49\cdot(453 - 3\cdot 124) = -179\cdot 124 + 49\cdot 453 \end{aligned}$$

Ainsi $-179\cdot 124 = 1\ [453]$.

- Soit $x \in \mathbb{Z}$.

$$\begin{aligned} 124\cdot x + 5 = 16\ [453] &\iff -179\cdot 124\cdot x - 179\cdot 5 = -179\cdot 16\ [453] \qquad [\times(-179) \text{ pour } \Rightarrow \text{ et } \times 124 \text{ pour } \Leftarrow] \\ &\iff x - 895 = -2\,864\ [453] \\ &\iff x = -1\,969\ [453] \\ &\iff x = 296\ [453] \end{aligned}$$

Dans ce qui précède, la première équivalence (le sens réciproque notamment) doit être analysée avec soin. L'ensemble solution de (E) est donc $\{296 + 453\cdot k\ :\ k \in \mathbb{Z}\}$.

C12.88. Lemme Soit p un nombre premier. Pour tout $k \in [\![1, p-1]\!]$, p divise $\binom{p}{k}$.

Démonstration

Soit $k \in [\![1, p-1]\!]$. Comme :

$$k\cdot\binom{p}{k} = p\cdot\binom{p-1}{k-1}$$

et $\binom{p-1}{k-1} \in \mathbb{N}$, p divise le produit $k\cdot\binom{p}{k}$. Comme p est premier, $p \wedge k = 1$ et le lemme de Gauß(C12.51) livre finalement p divise $\binom{p}{k}$.

C12.89. Théorème (petit théorème de Fermat) Soit p un nombre premier.

$$\forall a \in \mathbb{Z} \quad p \nmid a \implies a^{p-1} \equiv 1\ [p].$$

Démonstration

- Comme un entier est congru modulo n au reste de sa division euclidienne par n, il suffit de démontrer que, pour tout $r \in [\![1, p-1]\!]$, $r^{p-1} \equiv 1\ [p]$. Nous procédons par récurrence finie.
- *Initialisation* Si $r = 1$ alors $r^{p-1} = 1^{p-1} = 1$ et donc, *a fortiori*, $r^{p-1} \equiv 1\ [p]$. L'assertion est donc établie pour $r = 1$.
- *Hérédité* Soit $r \in [\![1, p-2]\!]$ tel que $r^{p-1} \equiv 1\ [p]$. D'après la formule du binôme de Newton :

$$(r+1)^p = \sum_{k=0}^{p} \binom{p}{k} r^k .$$

D'après le lemme C12.88 :

$$(\star) \qquad (r+1)^p \equiv r^p + 1\ [p] .$$

Comme $r^{p-1} \equiv 1\ [p]$, on a $r^p \equiv r\ [p]$ et donc $(\star)$ s'écrit encore :

$$(\star\star) \qquad (r+1)^p \equiv r+1\ [p] .$$

Comme $1 \leqslant r+1 \leqslant p-1$, $r+1$ est premier avec p. D'après C12.86, il existe $b \in \mathbb{Z}$ tel que $b \cdot (r+1) \equiv 1\ [p]$. En multipliant chaque membre de $(\star\star)$ par b, il vient :

$$(r+1)^{p-1} \equiv 1\ [p] .$$

C12.90. Exercice Quel est le reste de la division euclidienne de $5^{2\,023}$ par 7 ?

- Le nombre 7 est premier et 5 est premier avec 7. D'après le petit théorème de Fermat (C12.89) :

$$5^6 \equiv 1\ [7]$$

et donc pour tout $k \in \mathbb{N}$, $\left(5^6\right)^k \equiv 1\ [7]$, i.e.

$$5^{6k} \equiv 1\ [7]$$

- Nous calculons la division euclidienne de 2 023 par 6 : $2\,023 = 337 \cdot 6 + 1$.
- Ainsi :

$$\begin{aligned} 5^{2\,023} &\equiv 5^{337\cdot 6+1}\ [7] \\ &\equiv 5^{337\cdot 6} \cdot 5^1\ [7] \\ &\equiv 1 \cdot 5^1\ [7] \\ &\equiv 5\ [7] . \end{aligned}$$

- Nous en déduisons que le reste de la division euclidienne de $5^{2\,023}$ par 7 est 5.