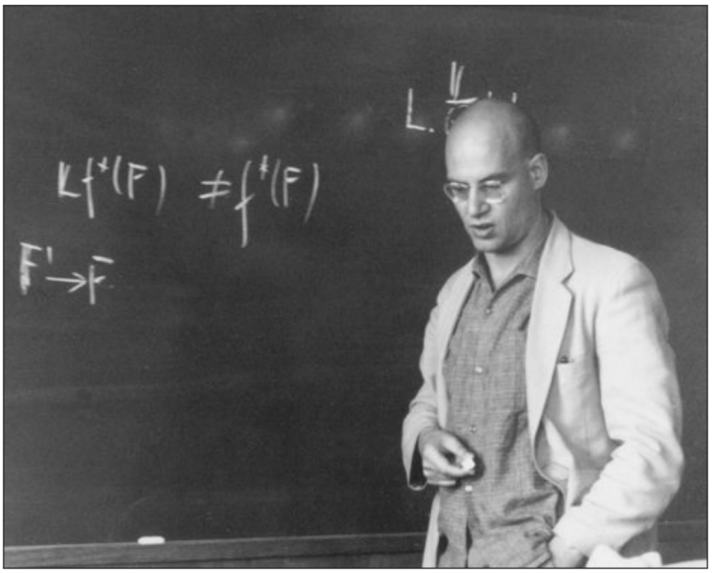
Chapitre 30

Arithmétique

Carl Friedrich Gauss
(1777 – 1855)



Alexandre Grothendieck
(1928 – 2014)

« Traditionnellement, on distingue trois types de "qualités" ou d'"aspects" des choses de l'Univers, qui soient objet de la réflexion mathématique : ce sont le ***nombre****,* ***la grandeur****, et la* ***forme****. On peut aussi les appeler l'aspect "****arithmétique****", l'aspect "****métrique****" (ou "analytique"), et l'aspect "****géométrique****" des choses. »*

Alexandre Grothendieck
Récoltes et semailles

L'arithmétique, c'est l'étude du nombre (et, en premier lieu, c'est l'étude des nombres entiers, des ensembles $\mathbb{N}$ *et* $\mathbb{Z}$*). Gauss disait de l'arithmétique que c'est la « reine des mathématiques ». Les nombreuses questions soulevées par cette discipline (par exemple, la preuve du théorème de Fermat, qui a tenu en échec les mathématiciens pendant plus de 350 ans) sont à l'origine de très nombreuses théories mathématiques.*

Sommaire

I. Diviseurs et multiples

1) Inversibles dans $\mathbb{Z}$

Remarque

Si A est un anneau, et si $x \in A$, on rappelle que x est dit *inversible (dans A)* $\overset{\Delta}{\text{ssi}}$

$$\exists y \in A : ab = ba = 1_A.$$

On note $A^\times$ ou $\mathrm{U}(A)$ l'ensemble des éléments inversibles de A.

Proposition ARI.1

Les inversibles de $\mathbb{Z}$ sont -1 et 1.

Démonstration. — .....

.....

.....

.....

..... ■

Exercice ARI.2

Montrer que

$$\forall k, k' \in \mathbb{Z},\ kk' = 1 \implies k = k'.$$

2) Division euclidienne

Théorème ARI.3

Soient $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$. Alors,

$$\exists!(q, r) \in \mathbb{Z} \times \mathbb{N} : \begin{cases} a = bq + r \\ 0 \leqslant r < b. \end{cases}$$

- *L'entier q est appelé* quotient de la division euclidienne de a par b.
- *L'entier r est appelé* reste de la division euclidienne de a par b.

Remarques

- L'entier a est appelé *dividende de la division euclidienne de a par b*.
- L'entier $b \neq 0$ est appelé *diviseur de la division euclidienne de a par b*.

Démonstration. — ⟶ Voir cours ■

3) Définition et exemples

Définition ARI.4
Soient $a, b \in \mathbb{Z}$.

- *On dit que* a divise b *et on note* $a \mid b$ $\overset{\Delta}{\text{ssi}}$

$$\exists k \in \mathbb{Z} : b = k \times a.$$

- *Dans ce cas, on dit aussi que* b est un multiple de a.
- *On note*

$$\mathsf{Div}(b) \coloneqq \Big\{ k \in \mathbb{Z} \mid k \text{ divise } b \Big\}.$$

Exemples

- On a $8 \mid 16$.
- On a $\forall n \in \mathbb{Z},\ 1 \mid n$ et $-1 \mid n$.
- Soit $n \in \mathbb{N}$. Si $0 \mid n$ alors $n = 0$.
- **Diviseurs de 0.**
  On a $\forall n \in \mathbb{Z},\ n \mid 0$. Donc,

$$\boxed{\mathsf{Div}(0) = \mathbb{Z}.}$$

- **Diviseurs de 1.**
  On a

$$\boxed{\mathsf{Div}(1) = \{-1, 1\}.}$$

4) Premières propriétés

Fait ARI.5
Soient $a, b \in \mathbb{Z}$.

1) *On suppose* $a \neq 0$. *Alors,*

$$a \mid b \iff \frac{b}{a} \in \mathbb{Z}.$$

2) *Soit* $k \in \mathbb{Z} \setminus \{0\}$. *Alors,*

$$a \mid b \iff ka \mid kb.$$

3) *Soit* $c \in \mathbb{Z}$. *Alors,*

$$a \mid b \implies a \mid bc.$$

Démonstration. — Elle est laissée au lecteur à titre d'entraînement. ■

5) Divisibilité et combinaisons linéaires

Proposition ARI.6
Soient $n, a, b \in \mathbb{Z}$. *Alors,*

$$\left.\begin{array}{l} n \mid a \\ n \mid b \end{array}\right\} \implies \forall (k, \ell) \in \mathbb{Z}^2,\ n \mid ka + \ell b.$$

Démonstration. — Elle est laissée au lecteur à titre d'entraînement. ■

6) La divisibilité est une relation de (pré)ordre

Proposition ARI.**7**
Soient $a, b, c \in \mathbb{Z}$. Alors,

- $a \mid a$;
- $\big(a \mid b \text{ et } b \mid a\big) \implies a = b \text{ ou } a = -b$;
- $\big(a \mid b \text{ et } b \mid c\big) \implies a \mid c$.

Démonstration. — Elle est laissée au lecteur à titre d'entraînement. ■

Remarques

- Ainsi, la relation « $\mid$ » de divisibilité est une relation d'ordre sur $\mathbb{N}$.
- C'est un préordre sur $\mathbb{Z}$.

7) Ordre et inégalité

Fait ARI.**8**
Soient $a, b \in \mathbb{Z}$. Alors,

$$\left.\begin{array}{l} a \mid b \\ b \neq 0 \end{array}\right\} \implies |a| \leqslant |b|.$$

Démonstration. — .....

.....

..... ■

II. PGCD et algorithme d'Euclide

1) Définition

Définition ARI.9
Soient $a, b \in \mathbb{N}$ avec $a \neq 0$ ou $b \neq 0$.

- *On appelle* pgcd de a et b *et on note* $\mathsf{pgcd}(a,b)$ *le plus grand entier $d \in \mathbb{Z}$ tel que $d \mid a$ et $d \mid b$.*
- *Autrement dit, on pose*
$$\mathsf{pgcd}(a,b) \coloneqq \mathsf{max}\Big\{ d \in \mathbb{Z} \;\Big|\; d \text{ divise } a \text{ et } b \Big\}.$$
- *Autrement dit, on pose*
$$\mathsf{pgcd}(a,b) \coloneqq \mathsf{max}\big(\mathsf{Div}(a) \cap \mathsf{Div}(b)\big).$$

Démonstration. —

- Supposons par exemple que $a \neq 0$.
- Alors, en vertu du fait ARI.8, $\mathsf{Div}(a)$ est majoré par a. Comme $1 \in \mathsf{Div}(a) \cap \mathsf{Div}(b)$, l'ensemble $\mathsf{Div}(a) \cap \mathsf{Div}(b)$ est une partie de $\mathbb{Z}$ non vide et majorée (par a) : elle possède un plus grand élément.

■

Remarques

- On note également $a \wedge b \coloneqq \mathsf{pgcd}(a,b)$.
- Évidemment, le PGCD de a et b est le plus grand diviseur commun entre a et b.
- En `Python`, pour calculer le PGCD de `a` et `b`, il faut importer le module `math` (`as mt` par exemple) et exécuter la commande `mt.gcd(a, b)`.
  En effet, en anglais, le PGCD se dit *greatest common divisor*.

Exercice ARI.10
Soient $a, b \in \mathbb{N}^*$ tels que $a \mid b$. Combien vaut $\mathsf{pgcd}(a,b)$?

Exercice ARI.11
Soit $a \in \mathbb{N}^*$. Combien vaut $\mathsf{pgcd}(a,0)$?

2) Présentation de l'algorithme d'Euclide

L'algorithme d'Euclide permet de calculer efficacement $\mathsf{pgcd}(a, b)$, en faisant des divisions euclidiennes et en considérant les restes successifs.

a) description de l'algorithme

Voici l'algorithme d'Euclide.

- On place a et b dans les deux premières lignes.
- On calcule le reste r et le quotient q de la division euclidienne de a par b.
- Puis, on reporte dans la ligne suivante :
  - ▷ le « b » de la ligne n devient le a de la ligne $n+1$;
  - ▷ le « r » de la ligne n devient le b de la ligne $n+1$.
- On continue jusqu'à ce que $r = 0$.
- Le PGCD est alors le dernier reste non nul.

a	b	r	q

b) pratique de l'algorithme sur un exemple

Calculons $\mathsf{pgcd}(1927, 2013)$.

a	b	r	q

Exercice ARI.12
Implémenter en `Python` *l'algorithme d'Euclide.*

3) Algorithme d'Euclide étendu

a) relations de Bézout

Définition ARI.13
Soit $(a,b) \in \mathbb{Z}^2 \setminus \{(0,0)\}$.
Une relation de Bézout entre a et b *est un couple* $(u,v) \in \mathbb{Z}^2$ *tel que*

$$au + bv = \mathsf{pgcd}(a,b).$$

Exemple

- Le PGCD entre 55 et 20 est 5.
- Une relation de Bézout entre 55 et 20 est

$$3 \times 55 - 8 \times 20 = 5.$$

b) description de l'algorithme

L'algorithme d'Euclide étendu permet de calculer le PGCD de a et b ainsi qu'une relation de Bézout. Le voici.

- On ajoute deux colonnes au tableau précédent pour u et v.
- On initialise ces deux colonnes avec les données :

u	v
1	0
0	1

- On remplit les quatre premières colonne de l'algorithme d'Euclide non étendu jusqu'au reste nul.
- On remplit ensuite les deux dernières colonnes à l'aide du motif :

	α
	β
q	$\alpha - q\beta$

- Les valeurs finales de u et v sur la ligne du dernier reste non nul vérifient alors

$$au + bv = \mathsf{pgcd}(a,b).$$

c) Pratique de l'algorithme sur un exemple

Calculons une relation de Bézout entre 2013 et 1927.

				u	v
				1	0
a	b	r	q	0	1

Remarques

- On remarque que u et v changent de signe à chaque ligne ; ceci peut être prouvé.
- De même, on remarque que les signes de u et v sont toujours opposés.
- Ces deux remarques peuvent aider à déceler des erreurs de calculs dans l'application de l'algorithme d'Euclide étendu.

Exercice ARI.**14**

Trouver une relation de Bézout entre votre année de naissance et 4 243.

Exercice ARI.**15**

Implémenter en `Python` *l'algorithme d'Euclide étendu.*

4) Preuve de l'algorithme d'Euclide étendu

a) Un lemme

Lemme ARI.**16**
Soient $a, b \in \mathbb{N}^*$.

1) *Soient* $q, r \in \mathbb{Z}$ *tels que* $\boxed{a = bq + r.}$ *Alors,* $\mathsf{pgcd}(a, b) = \mathsf{pgcd}(b, r)$.
2) *Soit* $r \in [\![0, b-1]\!]$ *le reste dans la division euclidienne de* a *par* b. *Alors,*

$$\mathsf{pgcd}(a, b) = \mathsf{pgcd}(b, r).$$

Démonstration. — .....

.....

.....

.....

.....

.....

.....

.....

.....

.....

..... ■

b) Description mathématique de l'algorithme

Soient $a, b \in \mathbb{N}^*$.

- On construit par récurrence les suites $(a_i)_i$, $(b_i)_i$, $(q_i)_i$ et $(r_i)_i$ de la façon suivante :
  - ▷ On pose $a_0 \coloneqq a$ et $b_0 \coloneqq b$.
  - ▷ Tant que $b_i \neq 0$, on effectue la division euclidienne de a_i par b_i, qu'on écrit

$$\boxed{a_i = b_i q_i + r_i.}$$

  - ▷ Puis, on pose $a_{i+1} \coloneqq b_i$ et $b_{i+1} \coloneqq r_i$.
- On a, par définition du reste dans la division euclidienne, $0 \leqslant r_i < b_i$, donc

$$0 \leqslant b_{i+1} < b_i.$$

Ainsi, d'après l'exercice qui suit, on peut affirmer que la suite $(b_i)_i$ finit par s'annuler.

Exercice ARI.**17**
Montrer qu'il n'existe pas de suite $(u_n)_{n\in\mathbb{N}}$ *strictement décroissante telle que* $\forall n \in \mathbb{N}$, $u_n \in \mathbb{N}$.

- Soit donc $N \in \mathbb{N}$ tel $b_N = 0$. On a donc $r_{N-1} = 0$, *ie* $\boxed{b_{N-1} \mid a_{N-1}.}$
- Donc, on a $\mathsf{pgcd}(a_{N-1}, b_{N-1}) = b_{N-1} = r_{N-2}$.

- Or, d'après le lemme ARI.16, comme on a $\forall i \in [\![0, N-1]\!],\ a_i = b_i q_i + r_i$, on a

$$\begin{aligned} &\forall i \in [\![0, N-1]\!],\ \mathsf{pgcd}(a_i, b_i) = \mathsf{pgcd}(b_i, r_i) \\ \text{donc}\quad &\forall i \in [\![0, N-1]\!],\ \mathsf{pgcd}(a_i, b_i) = \mathsf{pgcd}(a_{i+1}, b_{i+1}). \end{aligned}$$

- Ainsi, on a $\mathsf{pgcd}(a, b) = \mathsf{pgcd}(a_0, b_0) = \mathsf{pgcd}(a_{N-1}, b_{N-1}) = r_{N-2}$, qui est le dernier reste non nul.
- Pour résumer, $\boxed{\mathsf{pgcd}(a, b) = r_{N-2} = b_{N-1}.}$

5) Lecture matricielle de l'algorithme

Gardons les notations précédente.
Pour $i \in [\![0, N]\!]$, on a

$$\begin{cases} a_{i+1} = b_i \\ b_{i+1} = r_i = a_i - q_i b_i \end{cases}.$$

Ce qu'on peut écrire

$$\begin{pmatrix} a_{i+1} \\ b_{i+1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix} \begin{pmatrix} a_i \\ b_i \end{pmatrix}.$$

Donc, on a

$$\begin{aligned} \begin{pmatrix} a_{N-1} \\ b_{N-1} \end{pmatrix} &= \begin{pmatrix} 0 & 1 \\ 1 & -q_{N-2} \end{pmatrix} \begin{pmatrix} a_{N-2} \\ b_{N-2} \end{pmatrix} \\ &= \begin{pmatrix} 0 & 1 \\ 1 & -q_{N-2} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -q_{N-3} \end{pmatrix} \begin{pmatrix} a_{N-3} \\ b_{N-3} \end{pmatrix} \\ &= \begin{pmatrix} 0 & 1 \\ 1 & -q_{N-2} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -q_{N-3} \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & -q_0 \end{pmatrix} \begin{pmatrix} a_0 \\ b_0 \end{pmatrix} \end{aligned}$$

Notons $A \coloneqq \begin{pmatrix} 0 & 1 \\ 1 & -q_{N-2} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -q_{N-3} \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & -q_0 \end{pmatrix}$ et écrivons

$$A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}.$$

On a donc

$$\begin{pmatrix} a_{N-1} \\ b_{N-1} \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} a_0 \\ b_0 \end{pmatrix}$$

Comme on a $b_{N-1} = \mathsf{pgcd}(a, b)$, on en déduit

$$\boxed{\mathsf{pgcd}(a, b) = \gamma \times a + \delta \times b.}$$

Remarque

- Cette analyse matricielle permet de prouver la justesse de l'algorithme d'Euclide étendu.
- Notons $(u_i)_{i \geqslant -2}$ et $(v_i)_{i \geqslant -2}$ les coefficients des deux dernières colonnes. Notons également :

$$M_i \coloneqq \begin{pmatrix} u_i & v_i \\ u_{i+1} & v_{i+1}. \end{pmatrix}$$

Les relations de récurrence définissant les $(u_i)_{i \geqslant 2}$ et les $(v_i)_{i \geqslant 2}$ sont

$$\begin{cases} u_{i+1} = u_{i-1} - q_{i+1} u_i \\ v_{i+1} = v_{i-1} - q_{i+1} v_i \end{cases} \quad \text{et} \quad M_{-2} \coloneqq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2.$$

- Maintenant, calculons

$$\begin{aligned}\begin{pmatrix}0 & 1\\ 1 & -q_{i+2}\end{pmatrix}M_i &= \begin{pmatrix}0 & 1\\ 1 & -q_{i+2}\end{pmatrix}\begin{pmatrix}u_i & v_i\\ u_{i+1} & v_{i+1}\end{pmatrix}\\ &= \begin{pmatrix}u_{i+1} & v_{i+1}\\ u_i - q_{i+2}u_{i+1} & v_i - q_{i+2}v_{i+1}\end{pmatrix}\\ &= \begin{pmatrix}u_{i+1} & v_{i+1}\\ u_{i+2} & v_{i+2}\end{pmatrix}\\ &= M_{i+1}.\end{aligned}$$

- Donc,

$$\begin{aligned}A &= \begin{pmatrix}0 & 1\\ 1 & -q_{N-2}\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -q_{N-3}\end{pmatrix}\cdots\begin{pmatrix}0 & 1\\ 1 & -q_0\end{pmatrix}\\ &= \begin{pmatrix}0 & 1\\ 1 & -q_{N-2}\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -q_{N-3}\end{pmatrix}\cdots\underbrace{\begin{pmatrix}0 & 1\\ 1 & -q_0\end{pmatrix}\times M_{-2}}_{M_{-1}}\\ &= \begin{pmatrix}0 & 1\\ 1 & -q_{N-2}\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -q_{N-3}\end{pmatrix}\cdots\underbrace{\begin{pmatrix}0 & 1\\ 1 & -q_1\end{pmatrix}\times M_{-1}}_{M_0}\\ &= \cdots = \begin{pmatrix}0 & 1\\ 1 & -q_{N-2}\end{pmatrix}\times M_{N-4}\\ &= M_{N-3}\\ &= \begin{pmatrix}u_{N-3} & v_{N-3}\\ u_{N-2} & v_{N-2}\end{pmatrix}\end{aligned}$$

- Donc, on a

$$\boxed{\mathsf{pgcd}(a,b) = u_{N-2}\times a + v_{N-2}\times b}$$

les coefficients u_{N-2} et v_{N-2} étant ceux sur la ligne de r_{N-2}, le dernier reste non nul.

6) Théorème de Bachet-Bézout

Ainsi, on a montré

Théorème ARI.18 (Bachet-Bézout)
Soient $a, b \in \mathbb{N}^*$. Alors,

$$\exists u, v \in \mathbb{Z} :\ au + bv = \mathsf{pgcd}(a,b).$$

7) Le PGCD est aussi le plus grand diviseur commun pour la relation de divisibilité sur $\mathbb{N}$

Rappelons que la relation de divisibilité est une relation d'ordre sur $\mathbb{N}$. On dipose donc de deux relations d'ordre sur $\mathbb{N}$. On peut donc naturellement se poser la question : le PGCD est-il le plus grand diviseur commun pour ces deux relations d'ordre ?

- Par définition, il l'est pour $\leqslant$.
  Cela veut dire :
  $$\forall d \in \mathbb{N},\ \Big(d \mid a \text{ et } d \mid b\Big) \implies d \leqslant \mathsf{pgcd}(a,b).$$
- On va voir dans la proposition suivante que le PGCD l'est également pour la relation « $\mid$ » de divisibilité.
  Cela veut dire :
  $$\boxed{\forall d \in \mathbb{N},\ \Big(d \mid a \text{ et } d \mid b\Big) \implies d \mid \mathsf{pgcd}(a,b).}$$

Proposition ARI.19
Soient $a, b \in \mathbb{N}^*$ et soit $d \in \mathbb{Z}$. Alors, on a

$$\begin{cases} d \mid a \\ d \mid b \end{cases} \iff d \mid \mathsf{pgcd}(a,b).$$

Démonstration. — .....

.....

.....

.....

.....

.....

.....

..... ■

Remarques

- Cette proposition nous permet de donner un sens à $\mathsf{pgcd}(0,0)$.
- En effet, on a $\forall n \in \mathbb{Z}, n \mid 0$. Donc, $\mathsf{Div}(0) = \mathbb{N}$.
- Donc, le PGCD de 0 et 0 devrait être le plus grand élément de $\mathbb{N}$; évidemment, on sait que $\mathbb{N}$ ne possède pas de plus grand élément pour $\leqslant$.
- Cependant, comme on a
  $$\forall n \in \mathbb{Z},\ n \mid 0,$$
  cela veut dire que 0 est le plus grand élément de $\mathbb{N}$ pour la relation de divisibilité !
- Ainsi, en toute logique, on pose
  $$\boxed{\mathsf{pgcd}(0,0) \coloneqq 0.}$$
- De façon plus générale, si $a, b \in \mathbb{Z}$, on pose $\mathsf{pgcd}(a,b) \coloneqq \mathsf{pgcd}(|a|,|b|)$.

8) PGCD d'un nombre fini d'entiers

Soit $N \in \mathbb{N}^*$.

a) définition

Définition ARI.20

Soient $a_1, a_2, \dots, a_N \in \mathbb{Z}$ des entiers non tous nuls.
Le pgcd des entiers $a_1, a_2, \dots, a_N$, *noté* $\mathsf{pgcd}(a_1, a_2, \dots, a_N)$, *est le plus grand diviseur commun à tous les a_i.*

Remarques

- Autrement dit, dans ce cas, on pose
$$\mathsf{pgcd}(a_1, \dots, a_N) \coloneqq \max \bigcap_{i=1}^{N} \mathsf{Div}(a_i).$$
- De plus, on pose
$$\mathsf{pgcd}(0, \dots, 0) \coloneqq 0.$$

b) une réécriture

Lemme ARI.21

Soient $a_1, \dots, a_N \in \mathbb{Z}$. Alors,
$$\bigcap_{i=1}^{N} \mathsf{Div}(a_i) = \mathsf{Div}\Big(\cdots\Big(\big((a_1 \wedge a_2) \wedge a_3\big) \wedge a_4\Big) \wedge \cdots \wedge a_N\Big).$$

Exemple

- Écrivons ce lemme pour des petites valeurs de N pour le rendre plus lisible.
- Pour $N = 3$ et pour $a_1, a_2, a_3 \in \mathbb{Z}$, on a
$$\mathsf{Div}(a_1) \cap \mathsf{Div}(a_2) \cap \mathsf{Div}(a_3) = \mathsf{Div}\Big((a_1 \wedge a_2) \wedge a_3\Big).$$
- Pour $N = 4$ et pour $a_1, a_2, a_3, a_4 \in \mathbb{Z}$, on a
$$\mathsf{Div}(a_1) \cap \mathsf{Div}(a_2) \cap \mathsf{Div}(a_3) \cap \mathsf{Div}(a_4) = \mathsf{Div}\Big(\big((a_1 \wedge a_2) \wedge a_3\big) \wedge a_4\Big).$$

Démonstration. — On procède par récurrence sur N ; on note, pour $N \in \mathbb{N}^*$,
$$\mathscr{P}(N) : \text{« } \bigcap_{i=1}^{N} \mathsf{Div}(a_i) = \mathsf{Div}\Big(\Big(\cdots\Big(\big((a_1 \wedge a_2) \wedge a_3\big) \wedge a_4\Big) \wedge \cdots\Big) \wedge a_N\Big) \text{ ».}$$

- Si $N = 1$, c'est tautologique.
- Si $N = 2$, c'est la proposition ARI.19.
- Montrons maintenant l'hérédité. Soit $N \in \mathbb{N}^*$ tel que $\mathscr{P}(N)$. Montrons $\mathscr{P}(N+1)$.
Soient $a_1, \dots, a_{N+1} \in \mathbb{Z}$. Notons
$$\Delta \coloneqq \Big(\cdots\Big(\big((a_1 \wedge a_2) \wedge a_3\big) \wedge a_4\Big) \wedge \cdots\Big) \wedge a_N.$$
On raisonne par double-inclusion.

▷ • Soit $d \in \bigcap_{i=1}^{N+1} \mathsf{Div}(a_i)$.

• En particulier, on a $d \in \bigcap_{i=1}^{N} \mathsf{Div}(a_i)$. D'après $\mathscr{P}(N)$, on a donc $d \mid \Delta$.

• De plus, on a $d \mid a_{N+1}$.

• Donc, d'après la proposition ARI.19, on a $d \mid \mathsf{pgcd}(\Delta, a_{N+1})$, *ie* $d \in \mathsf{Div}\Big(\mathsf{pgcd}(\Delta, a_{N+1})\Big)$.

▷ Réciproquement, soit $d \in \mathsf{Div}\Big(\mathsf{pgcd}(\Delta, a_{N+1})\Big)$ *ie* soit $d \in \mathbb{Z}$ tel que $d \mid \mathsf{pgcd}(\Delta, a_{N+1})$. On a donc $d \mid \Delta$, *ie* $d \in \mathsf{Div}(\Delta)$. Donc, par hypothèse de récurrence, on a

$$d \in \bigcap_{i=1}^{N} \mathsf{Div}(a_i).$$

Comme on a aussi $d \mid a_{N+1}$, on a bien

$$d \in \bigcap_{i=1}^{N+1} \mathsf{Div}(a_i).$$

• Ainsi, on a bien

$$\bigcap_{i=1}^{N+1} \mathsf{Div}(a_i) = \mathsf{Div}\Big(\mathsf{pgcd}(\Delta, a_{N+1})\Big).$$

Autrement dit, $\mathscr{P}(N+1)$ est vrai.

• D'où l'hérédité et le résultat.

■

Corollaire ARI.**22**
Soient $a_1, \dots, a_N \in \mathbb{Z}$. Alors,

$$\mathsf{pgcd}(a_1, \dots, a_N) = \Big(\cdots\Big(\big((a_1 \wedge a_2) \wedge a_3\big) \wedge a_4\Big) \wedge \cdots\Big) \wedge a_N.$$

Démonstration. — C'est une conséquence du lemme précédent. On laisse le lecteur qui le souhaite le rédiger, en faisant attention aux a_i qui sont nuls. ■

c) associativité

Proposition ARI.**23**
Soient $a_1, \dots, a_{N+1} \in \mathbb{Z}$. Alors,

$$\mathsf{pgcd}(a_1, \dots, a_{N+1}) = \mathsf{pgcd}\Big(\mathsf{pgcd}(a_1, \dots, a_N),\, a_{N+1}\Big).$$

Démonstration. — C'est une conséquence immédiate du corollaire ARI.22. ■

d) relation de Bézout

Théorème ARI.**24**
Soient $a_1, \dots, a_N \in \mathbb{Z}$. Alors,

$$\exists (k_1, \dots, k_N) \in \mathbb{Z}^N : \quad k_1 a_1 + \cdots + k_N a_N = \mathsf{pgcd}(a_1, \dots, a_N).$$

Remarques

- Un tel N-uplet est appelé *relation de Bézout* entre pour la famille $(a_1, \dots, a_N)$.
- Il faut retenir que ce résultat est très puissant et permet de prouver de nombreuses choses.

Démonstration. — Il suffit d'utiliser la proposition ARI.23, de procéder par récurrence en s'appuyant sur le théorème ARI.18. On laisse au lecteur regarder les détails pour vérifier qu'il a bien compris le mécanisme de la preuve. ■

Exercice ARI.**25**

1) *Calculer le PGCD de* 12, 15 *et* 30.
2) *Déterminer une relation de Bézout entre* 12, 15 *et* 30.

e) propriété fondamentale

Proposition ARI.**26**
Soient $a_1, \dots, a_N \in \mathbb{Z}$. Alors, pour tout $d \in \mathbb{Z}$, on

$$d \mid \mathsf{pgcd}(a_1, \dots, a_N) \quad \iff \quad \forall i \in [\![1, N]\!],\ d \mid a_i$$

Démonstration. —

- $\boxed{\implies}$ C'est le sens facile. On laisse le lecteur le vérifier.
- $\boxed{\impliedby}$ On suppose que $\forall i \in [\![1, N]\!],\ d \mid a_i$. On a donc

$$\forall (\lambda_i)_i \in \mathbb{Z}^N,\ \ d \ \mid \ \sum_{i=1}^{N} \lambda_i a_i.$$

Maintenant, on se donne une relation de Bézout $(k_1, \dots, k_N)$ de la famille $(a_1, \dots, a_N)$. On a ainsi

$$d \ \mid \ \sum_{i=1}^{N} k_i a_i \quad \text{donc} \quad d \mid \mathsf{pgcd}(a_1, \dots, a_N).$$

■

Remarques

- Autrement dit, le PGCD est également le plus grand des diviseurs communs aux a_i pour la relation de divisibilité.
- Cela justifie *a posteriori* la convention $\mathsf{pgcd}(0, \dots, 0) := 0$.

III. Nombres premiers entre eux

1) Définition : cas de deux entiers

Définition ARI. **27**
Soient $a, b \in \mathbb{Z}$. *On dit que* a et b sont premiers entre eux $\overset{\Delta}{\text{ssi}}$ $\mathsf{pgcd}(a, b) = 1$.

Exemples

- 12 et 15 ne sont pas premiers entre eux.
- 7 et 20 sont premiers entre eux.

2) Définition : cas de N entiers

Soient $a_1, \ldots, a_N \in \mathbb{Z}$.

a) entiers deux-à-deux premiers entre eux

Définition ARI. **28**
On dit que $a_1, \ldots, a_N$ sont deux-à-deux premiers entre eux $\overset{\Delta}{\text{ssi}}$

$$\forall i, j \in [\![1, N]\!], \qquad i \neq j \implies \mathsf{pgcd}(a_i, a_j) = 1.$$

Exemples

- Les entiers 15, 8 et 49 sont deux-à-deux premiers entre eux. En effet, on a $15 \wedge 8 = 1$, $15 \wedge 49 = 1$ et $8 \wedge 49 = 1$.
- En revanche, les entiers 15, 12 et 4 ne sont pas deux-à-deux premiers entre eux. En effet, on a $15 \wedge 12 = 3$. On aurait aussi pu remarquer que $12 \wedge 4 = 4$.

b) entiers premiers entre eux dans leur ensemble

Définition ARI. **29**
On dit que $a_1, \ldots, a_N$ sont premiers entre eux dans leur ensemble $\overset{\Delta}{\text{ssi}}$

$$\mathsf{pgcd}(a_1, \ldots, a_N) = 1.$$

Exemple

Les entiers 15, 12 et 4 sont premiers entre eux dans leur ensemble. En effet,

$$\mathsf{pgcd}(15, 12, 4) = \mathsf{pgcd}\Big(\mathsf{pgcd}(15, 12), 4\Big) = \mathsf{pgcd}(3, 4) = 1.$$

Proposition ARI.**30**
Soient $a_1, \dots, a_N \in \mathbb{Z}$. On a

$$a_1, \dots, a_N \text{ deux-à-deux premiers entre eux}$$
$$\Downarrow$$
$$a_1, \dots, a_N \text{ premiers entre eux dans leur ensemble.}$$

Démonstration. — Supposons par exemple que $a_1 \wedge a_2 = 1$.
On a vu que

$$\mathsf{pgcd}(a_1, \dots, a_N) = \Big(\cdots \Big(\big(\underbrace{(a_1 \wedge a_2)}_{=1} \wedge a_3 \big) \wedge a_4 \Big) \Big) \cdots \wedge a_N.$$

On en déduit que $\mathsf{pgcd}(a_1, \dots, a_N) = 1$. ■

3) Théorème de Bézout

Théorème ARI.**31**
Soient $a, b \in \mathbb{Z}$. Alors,

$$a \text{ et } b \text{ premiers entre eux} \iff \exists (k, \ell) \in \mathbb{Z}^2 : \ ka + \ell b = 1.$$

Démonstration. —

- $\boxed{\Longrightarrow}$ C'est une conséquence du théorème ARI.18.
- $\boxed{\Longleftarrow}$ Supposons $\exists (k, \ell) \in \mathbb{Z}^2 : \ ka + \ell b = 1$ et fixons k et ℓ deux tels entiers.
  Soit d divisant a et b. Alors, d divise tout combinaison linéaire de a et b. Donc,

  $$d \mid ka + \ell b \quad \text{donc} \quad d \mid 1.$$

  Donc, $\mathsf{pgcd}(a, b) = 1$.

■

4) Lemme de Gauss

a) le lemme de Gauss

Théorème ARI.**32**
Soient $a, b, c \in \mathbb{Z}$. Alors,

$$\left.\begin{array}{l} a \mid bc \\ a \wedge b = 1 \end{array}\right\} \implies a \mid c.$$

Démonstration. — .....

.....

.....

.....

.....

.....

..... ■

b) conséquences

Proposition ARI.**33**
Soient $a, b \in \mathbb{Z}$ et soit $n \in \mathbb{Z}$. Alors,

$$\left.\begin{array}{ll} a \mid n & et \quad b \mid n \\ a \wedge b = 1 & \end{array}\right\} \implies ab \mid n.$$

Démonstration. — .....

.....

.....

.....

.....

.....

..... ■

Proposition ARI.**34**
Soient $a, b \in \mathbb{Z}$ et soit $n \in \mathbb{Z}$. Alors,

$$\left.\begin{array}{l} a \wedge n \\ b \wedge n \end{array}\right\} \implies ab \wedge n.$$

Démonstration. — .....

.....

.....

.....

.....

.....

..... ■

IV. Nombres premiers

1) Définition

Définition ARI.35

- *Soit $p \in \mathbb{N}$. On dit que p* est premier $\overset{\Delta}{\text{ssi}}$ *p possède exactement deux diviseurs dans $\mathbb{N}$.*
- *On note $\mathscr{P}$ l'ensemble des nombres premiers.*
- *Un nombre $n \in \mathbb{Z} \setminus \{0, 1, -1\}$ qui n'est pas premier est dit* composé.

Remarque

- On a donc
$$p \text{ est premier} \iff \Big(\mathrm{Div}(p) \cap \mathbb{N} \text{ fini} \quad \text{et} \quad \big|\mathrm{Div}(p) \cap \mathbb{N}\big| = 2\Big).$$

Exemples

- On a $\boxed{1 \notin \mathscr{P}}$ car $\big|\mathrm{Div}(p) \cap \mathbb{N}\big| = 1$.
- Voilà la liste des premiers nombres premiers :
$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31 \in \mathscr{P}.$$
- En revanche, $91 \notin \mathscr{P}$. En effet, $91 = 7 \times 13$.

Remarque

Déterminer si, oui ou non, un nombre $n \in \mathscr{P}$ et, si non, trouver une factorisation de n est un problème algorithmique compliqué. C'est sur la difficulté de factoriser un nombre composé qu'est construite toute la sécurité des échanges de données en informatique.

2) Lemme d'Ératosthène

Lemme ARI.36 (d'Ératosthène)
Soit $N \in \mathbb{N}_{\geqslant 2}$ un nombre composé. Alors,
$$\exists p \in \mathscr{P} : \quad \Big(p \mid N \quad et \quad p \leqslant \big\lfloor \sqrt{N} \big\rfloor\Big).$$

Démonstration. — .....

.....

.....

.....

.....

.....

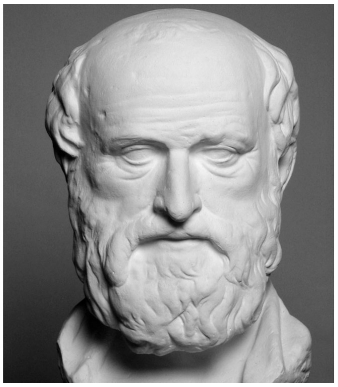
.....

.....

.....

.....

3) Crible d'Ératosthène



Ératosthène de Cyrène (276 av. JC – 194 av. JC)

a) Description de l'algorithme

Soit $N \in \mathbb{N}_{\geqslant 2}$.
Pour déterminer les nombres premiers inférieurs ou égaux à N, on procède comme suit :

1) On détermine les nombres premiers $p_1, p_2, \ldots, p_\ell$ inférieurs ou égaux à $\left\lfloor \sqrt{N} \right\rfloor$.
2) On exclut de $[\![2, N]\!]$ tous les multiples de $p_1, p_2, \ldots, p_\ell$.
3) Les nombres restants sont exactement les nombres premiers inférieurs ou égaux à N.

Cet algorithme est donc naturellement récursif.

b) Détermination des premiers nombres premiers

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

4) L'ensemble $\mathscr{P}$ est infini

Théorème ARI.**37** (Euclide)
$\mathscr{P}$ est infini.

Démonstration. — On raisonne par l'absurde et on écrit

$$\mathscr{P} = \Big\{p_1, p_2, \dots, p_m\Big\},$$

avec $p_1 < p_2 < p_3 < \cdots < p_m$. On considère alors $N \coloneqq p_1 \times p_2 \times \cdots \times p_m + 1$. Comme $\forall j,\ p_j \geqslant 1$, on a

$$p_1 \times p_2 \times \cdots \times p_m \geqslant p_m > p_k$$

pour tout $k \in [\![1, m]\!]$. En particulier, N n'est égal à aucun des p_k. Donc, $N \notin \mathscr{P}$.
Ainsi, d'après le lemme d'Ératosthène, N possède un diviseur premier. Soit donc $k \in [\![1, m]\!]$ tel que $p_k \mid N$.
Ainsi, on a

$$\left.\begin{array}{l} p_k \mid N \\ p_k \mid p_1 \times p_2 \times \cdots \times p_m \end{array}\right\} \text{ donc } p_k \mid (N - p_1 \times p_2 \times \cdots \times p_m).$$

Donc $p_k \mid 1$. Donc, $p_k \in \{\pm 1\}$. C'est absurde. ■

5) Décomposition en produit de nombres premiers

a) L'énoncé

Théorème ARI.**38**
Tout entier $n \geqslant 2$ s'écrit de façon unique (à l'ordre près des facteurs) comme produit de nombres premiers.

Démonstration. — ⟶ Voir cours ■

Exemples

- On a $42 = 6 \times 7 = 2 \times 3 \times 7$.
- On a $1\,729 = 7 \times 13 \times 19$.
- On a $1\,515 = 3 \times 5 \times 101$.
- On a

$$\begin{aligned} 840 &= 2 \times 420 \\ &= 2^2 \times 210 \\ &= 2^3 \times 105 \\ &= 2^3 \times 5 \times 21 \\ &= 2^3 \times 5 \times 3 \times 7 \\ &= \boxed{2^3 \times 3 \times 5 \times 7.} \end{aligned}$$

b) Algorithme

Voici un algorithme pour déterminer la décomposition en facteurs premiers d'un entier.
Soit $n \in \mathbb{N}$.

1) Si $n \in \mathscr{P}$ (grâce à l'algorithme d'Ératosthène) : c'est terminé.
2) a) Sinon, le crible d'Ératosthène nous donne un nombre premier p tel que $p \mid n$.
   b) On écrit $n = p \times m$ et on réapplique cet algorithme à m.

Exercice ARI.39
Implémenter cet algorithme en `Python`.

6) Valuations p-adiques

a) Définition

Définition ARI.40
Soit $n \in \mathbb{Z} \setminus \{0\}$ et soit $p \in \mathscr{P}$.
La valuation p-adique de n, *notée $v_p(n)$, est le plus grand entier $k \in \mathbb{N}$ tel que p^k divise n.*
Ie, *on pose*

$$v_p(n) \coloneqq \max\left\{k \in \mathbb{N} \;\middle|\; p^k \text{ divise } n\right\}.$$

Dit autrement, la valuation p-adique d'un entier n est la puissance à laquelle est élevé p dans la décomposition en facteurs premiers de n.

Exercice ARI.41
Soient $p \in \mathscr{P}$ et $n \in \mathbb{Z} \setminus \{0\}$. On note

$$A \coloneqq \left\{k \in \mathbb{N} \;\middle|\; p^k \text{ divise } n\right\}.$$

1) *Montrer que A est non vide.*
2) *Montrer que A est majoré.*

Exemples

- $v_2(60) = 2$
- $v_2(1024) = 10$
- $v_3(105) = 1$

⟶ Voir cours

Remarque

Par convention, on pose $v_p(0) = +\infty$ pour tout nombre premier p. Cette convention est cohérente puisque tous les entiers divisent 0 et qu'on a donc

$$\left\{k \in \mathbb{N} \;\middle|\; p^k \text{ divise } 0\right\} = \mathbb{N}.$$

b) Valuation p-adique et décomposition en facteurs premiers

Soit $n \geqslant 2$. On décompose n en produit de nombres premiers en écrivant

$$n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}.$$

avec les p_i des nombres premiers deux à deux distincts et avec $\forall i, \alpha_i \in \mathbb{N}^*$.

- On peut déjà remarquer que les seuls nombres premiers p qui divisent n sont les p_i.
- De plus, on a
$$\forall i \in [\![1, r]\!],\ v_{p_i}(n) = \alpha_i.$$
De plus, si p ne divise pas n, on a $v_p(n) = 0$.
- Ainsi, on peut écrire
$$n = \prod_{\substack{p \in \mathscr{P} \\ p|n}} p^{v_p(n)}.$$
- De plus, si $p \nmid n$, on a $v_p(n) = 0$ et donc $p^{v_p(n)} = p^0 = 1$. Ainsi, on peut écrire :

Théorème ARI.**42**
Soit $n \in \mathbb{N}_{\geqslant 1}$. On a

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

c) Valuation p-adique du produit et de la somme

Proposition ARI.**43**
Soient $n, m \in \mathbb{Z}$ et soit $p \in \mathscr{P}$. On a

1) $v_p(n \times m) = v_p(n) + v_p(m)$;
2) $v_p(n + m) \geqslant \min\big(v_p(n), v_p(m)\big)$.

Démonstration. — ⟶ Voir cours ■

d) Valuation p-adique et divisibilité

Proposition ARI.**44**
Soient $n, m \in \mathbb{Z}$. On a

$$n \mid m \iff \forall p \in \mathscr{P},\ v_p(n) \leqslant v_p(m).$$

Démonstration. — ⟶ Voir cours ■

Exercice ARI.**45**
Soit $n \in \mathbb{N}_{\geqslant 2}$. Combien n possède-t-il de diviseurs ?

7) PGCD et valuation p-adique

Proposition ARI.46
Soient $a, b \in \mathbb{N}^*$. Alors, on a

$$\mathsf{pgcd}(a,b) = \prod_{p \in \mathscr{P}} p^{\min(v_p(a), v_p(b))}.$$

Démonstration. — ⟶ Voir cours ■

Exemples

- Calculons $\mathsf{pgcd}(27, 105)$.
  - ▷ On a $27 = 3^3$.
  - ▷ On a $105 = 3 \times 5 \times 7$.

  Donc, on a $\mathsf{pgcd}(27, 105) = 3^{\min(3,1)} \times 5^{\min(0,1)} \times 7^{\min(0,1)} = 3$.
- Calculons $\mathsf{pgcd}(2020, 4243)$ ⟶ Voir cours

On voit que cette méthode du calcul du PGCD n'est réalisable que si les entiers a et b sont petits ou que l'on connaît leurs décompositions en facteurs premiers.

V. Congruences

1) Définition

Définition ARI.47
Soit $n \in \mathbb{N}^*$ et soient $a, b \in \mathbb{Z}$.
On dit que a et b sont congrus modulo *n et on note $a \equiv b\ [n]$* $\overset{\Delta}{\text{ssi}}$

$$n \mid a - b.$$

Exemples

- La congruence modulo 2 traduit la parité. Ainsi, si $a, b \in \mathbb{Z}$, on a

$$a \equiv 0\ [2] \iff a \text{ pair}$$
$$a \equiv 1\ [2] \iff a \text{ impair}$$
$$a \equiv b\ [2] \iff a \text{ et } b \text{ ont même parité.}$$

- Si $n \in \mathbb{N}^*$, on a toujours

$$n \equiv 0\ [n].$$

Exercice ARI.48
Soit $a \in \mathbb{Z}$. On note $\mathsf{reste}_n(a)$ le reste de a dans sa division euclidienne modulo n.
Montrer que

$$a \equiv b\ [n] \iff \mathsf{reste}_n(a) = \mathsf{reste}_n(b).$$

2) La congruence modulo n est une relation d'équivalence

a) c'est une relation d'équivalence

Proposition ARI.49
La relation « être congru modulo n » est une relation d'équivalence.

Démonstration. — Elle est laissée au lecteur à titre d'entraînement. ■

b) l'ensemble $\mathbb{Z}/n\mathbb{Z}$

Si $a \in \mathbb{Z}$, on note $[a]_n$ la classe d'équivalence de a pour la relation « être congru modulo n » ; on a donc

$$[a]_n \coloneqq \Big\{ k \in \mathbb{Z} \;\Big|\; k \equiv a \ [n] \Big\}.$$

On a ainsi $[0]_n = n\mathbb{Z}$ et (par exemple)

$$[1]_n = \Big\{ \ldots, 1-3n, 1-2n, 1-n, 1, 1+n, 1+2n, 1+3n, \ldots \Big\} = 1 + n\mathbb{Z}.$$

Lemme ARI.50
Pour tout $a \in \mathbb{Z}$, il existe $r \in [\![0, n-1]\!]$ tel que $[a]_n = [r]_n$.
Autrement dit, on a

$$\Big\{ [a]_n \ ; \ a \in \mathbb{Z} \Big\} = \Big\{ [0]_n, [1]_n, \ldots, [n-1]_n \Big\}.$$

Démonstration. — Elle est laissée au lecteur à titre d'entraînement. ■

Définition ARI.51
L'ensemble $\mathbb{Z}$ sur $n\mathbb{Z}$, noté $\mathbb{Z}/n\mathbb{Z}$, est

$$\boxed{\mathbb{Z}/n\mathbb{Z} \coloneqq \Big\{ [a]_n \ ; \ a \in \mathbb{Z} \Big\} = \Big\{ [0]_n, [1]_n, \ldots, [n-1]_n \Big\}.}$$

Remarques

- L'ensemble $\mathbb{Z}/n\mathbb{Z}$ est fini de cardinal n.
- On peut le munir de deux lois $+$ et $\times$ définies par

$$[a]_n + [n-1]_b \coloneqq [n-1]_{a+b}$$
$$[a]_n \times [n-1]_b \coloneqq [n-1]_{a \times b}$$

  pour tous $a, b \in \mathbb{Z}$.
- Pour que ces définitions ait un sens, il faut montrer que le résultat $[n-1]_{a+b}$ ne dépendent pas du a et du b choisis représentant $[a]_n$ et $[n-1]_b$. De même pour la loi $\times$.
- On obtient alors un anneau commutatif

$$\Big(\mathbb{Z}/n\mathbb{Z}, +, \times, [0]_n, [1]_n\Big).$$

3) Congruences et opérations

Soient $a, b \in \mathbb{Z}$ et $\alpha, \beta \in \mathbb{Z}$.

a) congruence et somme

Lemme ARI.**52**
On a

$$\left.\begin{array}{l} a \equiv \alpha\ [n] \\ b \equiv \beta\ [n] \end{array}\right\} \implies a + b \equiv \alpha + \beta\ [n].$$

Démonstration. — Elle est laissée au lecteur à titre d'entraînement. ■

b) congruence et produit

Proposition ARI.**53**
On a

$$\left.\begin{array}{l} a \equiv \alpha\ [n] \\ b \equiv \beta\ [n] \end{array}\right\} \implies a \times b \equiv \alpha \times \beta\ [n].$$

Démonstration. — .....

.....

..... ■

c) congruence et puissance

Proposition ARI.**54**
On a

$$a \equiv \alpha\ [n] \implies \big(\forall k \in \mathbb{N},\ a^k \equiv \alpha^k\ [n]\big).$$

Démonstration. — On raisonne par récurrence et on utilise la proposition ARI.53. ■

4) Inverses d'un entier modulo n

a) définition

Définition ARI.**55**
Soit $a \in \mathbb{Z}$.

1) *Soit $\alpha \in \mathbb{Z}$. On dit que α* est un inverse de a modulo n $a\alpha \equiv 1\ [n]$.
2) *On dit que a* est inversible modulo n $\overset{\Delta}{\text{ssi}}$

$$\exists \alpha \in \mathbb{Z} :\ \alpha \text{ est un inverse } a \text{ modulo } n.$$

Exemples

- On a $3 \times 5 = 15 \equiv -1\ [4]$ donc $3 \times (-5) \equiv 1\ [4]$. Ainsi : 3 est inversible modulo 4 et -5 est un inverse de 3 modulo 4.
- Montrons que 5 n'est pas inversible modulo 100.
  Supposons le contraire et fixons $b \in \mathbb{Z}$ tel que $5b \equiv 1\ [100]$. On aurait alors, en multipliant par 20 : $100b \equiv 20\ [100]$ et donc $0 \equiv 20\ [100]$, ce qui absurde.

Remarque

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

$$a \text{ inversible modulo } n \iff [a]_n \in \mathrm{U}(\mathbb{Z}/n\mathbb{Z}).$$

On laisse le lecteur le démontrer. C'est un très bon exercice.

b) unicité modulo n de l'inverse modulo n

Proposition ARI.**56**

Soit $a \in \mathbb{Z}$ et soient $\alpha, \alpha' \in \mathbb{Z}$. Alors,

$$\left.\begin{array}{l} \alpha \text{ inverse de } a \text{ modulo } n \\ \alpha' \text{ inverse de } a \text{ modulo } n \end{array}\right\} \implies \alpha \equiv \alpha' \ [n].$$

Démonstration. — .....

.....

.....

..... ■

c) caractérisation des entiers inversibles modulo n

Proposition ARI.**57**

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

1) *on a*

$$a \text{ inversible modulo } n \iff \mathsf{pgcd}(a, n) = 1.$$

2) *Plus précisément si $(k, \ell) \in \mathbb{Z}^2$ vérifie $ak + n\ell = 1$, alors k est un inverse de a modulo n.*

Démonstration. — .....

.....

.....

.....

.....

.....

.....

.....

.....

..... ■

d) utilisation des entiers inversibles modulo n

Proposition ARI.**58**
Soit $a \in \mathbb{Z}$ inversible modulo n dont α est un inverse modulo n. Alors,

1) *pour tous $x, y \in \mathbb{Z}$,*
$$ax \equiv ay\ [n] \quad \Longrightarrow \quad x \equiv y\ [n].$$

2) *pour tous $x, b \in \mathbb{Z}$,*
$$ax \equiv b\ [n] \quad \Longleftrightarrow \quad x \equiv \alpha b\ [n].$$

Démonstration. — Elle est laissée au lecteur à titre d'entraînement. ■

5) Petit théorème de Fermat

Théorème ARI.**59**
Soit p un nombre premier et soit $n \in \mathbb{Z}$.

1) *On a*
$$\boxed{n \wedge p = 1 \quad \Longrightarrow \quad n^{p-1} \equiv 1\ [p].}$$

2) *En particulier, on a*
$$\boxed{n^p \equiv n\ [p].}$$

Démonstration. — ⟶ Voir cours ■

VI. PPCM

1) Définition

On définit le PPCM entre deux entiers $a, b \in \mathbb{N}^*$ comme on a défini le PGCD.
On le note $\mathsf{ppcm}(a, b)$ ou $a \vee b$.

2) PPCM et valuation p-adique

Proposition ARI.**60**
Soient $a, b \in \mathbb{N}^*$. Alors,
$$\mathsf{ppcm}(a, b) = \prod_{p \in \mathscr{P}} p^{\mathsf{max}(v_p(a), v_p(b))}.$$

Corollaire ARI.**61**
Soient $a, b \in \mathbb{N}^*$. Alors,
$$\mathsf{ppcm}(a, b) \times \mathsf{pgcd}(a, b) = a \times b.$$

3) Être multiple commun équivaut à être multiple du PPCM

Proposition ARI.**62**
Soient $a, b \in \mathbb{N}^*$ et soit $n \in \mathbb{Z}$. Alors, on a
$$\begin{cases} a \mid n \\ b \mid n \end{cases} \iff \mathsf{ppcm}(a, b) \mid n.$$