Chapitre I - D'où l'on parle

1. Arithmétique élémentaire
2. Calculer en (grands) nombres entiers
3. Description des structures : monoïde, groupe, anneau, corps
4. Des flèches et des morphismes
5. $\mathbb{N}$ à partir de Péano-Dedekind
6. $\mathbb{Z}$ comme extension de $\mathbb{N}$

1. Arithmétique élémentaire

1. Division euclidienne
2. ppcm, pgcd
3. Bézout et l'algorithme d'Euclide étendu
4. Lemme de Gauss, et quelques autres conséquences de Bézout
5. Nombres premiers et théorème fondamental de l'arithmétique (TFA)

Euclide (environ -300, époque de Ptolémée I)
Claude-Gaspard Bachet, sieur de Méziriac (1581-1638) : traduit en latin l'**Arithmetica** de Diophante (150-350 ? ? ?) ...
Etienne Bézout (1730-1783)
Carl Friedrich Gauss (1777-1855) : **Disquisitiones arithmeticæ** (1801)

1. Division euclidienne

Théorème (division euclidienne)

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

$$a = bq + r \quad et \quad 0 \leq r < b$$

Démonstration : exercice. □

Définition (multiple, diviseur)

Soient $a, b \in \mathbb{N}$. S'il existe $q \in \mathbb{N}$ tel que $a = bq$, on dit, selon l'humeur, que :

- a est multiple de b,
- b est un diviseur de a,
- b divise a, et on note : $b|a$.

2. ppcm, . . .

Soient des entiers $x_1, \ldots, x_n \in \mathbb{N}$.

Définition (ppcm)

$m \in \mathbb{N}$ est un plus petit commun multiple des $x_1, \ldots, x_n$ si

1. m est multiple commun aux $x_1, \ldots, x_n$, *i.e.*

$$(\forall j \in [\![1, n]\!]) \qquad x_j | m$$

2. si m' est un autre multiple commun aux $x_1, \ldots, x_n$, alors $m | m'$.

On note : $m = \mathrm{ppcm}(x_1, \ldots, x_n)$.

Exercices :

1. Le seul multiple de 0 est 0. 0 est multiple de tout entier $n \in \mathbb{N}$.
2. $\mathrm{ppcm}(x_1, \ldots, x_n) = 0 \iff (\exists j \in [\![1, n]\!]) \quad x_j = 0.$
3. existence et unicité du ppcm ?
4. $\mathrm{ppcm}(\mathrm{ppcm}(a, b), c) = \mathrm{ppcm}(a, b, c)$

. . . et pgcd

Soient des entiers $x_1, \ldots, x_n \in \mathbb{N}$.

Définition (pgcd)

$d \in \mathbb{N}$ est un plus grand commun diviseur des $x_1, \ldots, x_n$ si

1. d est un diviseur commun aux $x_1, \ldots, x_n$, *i.e.*

$$(\forall j \in [\![1, n]\!]) \qquad d | x_j$$

2. si d' est un autre diviseur commun aux $x_1, \ldots, x_n$, alors $d' | d$.

On note : $d = \mathrm{pgcd}(x_1, \ldots, x_n)$.

Exercice : $\mathrm{pgcd}(\mathrm{pgcd}(a, b), c) = \mathrm{pgcd}(a, b, c)$

Définition (entiers premiers entre eux)

Les entiers $x_1, \ldots, x_n$ sont dits premiers entre eux, ou étrangers, si $\mathrm{pgcd}(x_1, \ldots, x_n) = 1$.

3. Bézout et l'algorithme d'Euclide étendu

Théorème (Bézout)

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

1. $pgcd(a,b) = d \implies \exists u, v \in \mathbb{Z}, \quad d = ua + vb$
2. $pgcd(a,b) = 1 \iff \exists u, v \in \mathbb{Z}, \quad 1 = ua + vb$

Démonstration : constructive par l'algorithme d'Euclide étendu.
Supposons $b \leq a$ et posons :

$$\begin{cases} r_0 = a \\ r_1 = b \end{cases} ; \quad \begin{cases} u_0 = 1 \\ u_1 = 0 \end{cases} ; \quad \begin{cases} v_0 = 0 \\ v_1 = 1 \end{cases}$$

puis calculons, $\forall k \geq 1$ et tant que $r_{k+1} \neq 0$,

$$\begin{cases} r_{k-1} = r_k q_k + r_{k+1} & (\text{division euclidienne de } r_{k-1} \text{ par } r_k) \\ u_{k+1} = u_{k-1} - q_k u_k \\ v_{k+1} = v_{k-1} - q_k v_k \end{cases}$$

Bézout et l'algorithme d'Euclide étendu (2)

• **L' algorithme d'Euclide étendu s'arrête . . .**
sinon, la suite des restes r_k serait une suite strictement décroissante de $\mathbb{N}$, ce qui est impossible. Il existe donc un entier $n \geq 1$ tel que $r_{n+1} = 0$.
• **sur un résultat correct.**
On exhibe ces deux invariants de boucle :

$$\begin{array}{lrcl} \forall k \geq 0, & \operatorname{pgcd}(r_k, r_{k+1}) & = & \operatorname{pgcd}(a, b) \\ & r_k & = & u_k a + v_k b \end{array}$$

A l'arrêt de l'algorithme (*i.e.* $k = n$ tel que $r_{n+1} = 0$) on a donc :

$$\left\{ \begin{array}{rcl} r_n & = & \operatorname{pgcd}(a, b) \\ r_n & = & u_n a + v_n b \end{array} \right.$$

□

4. Lemme de Gauss, et autres conséquences de Bézout

Exercices :

1. $(c|a \text{ et } c|b) \Longrightarrow c|\text{pgcd}(a,b)$
2. $\big(a = da',\ b = db' \text{ avec } a' \wedge b' = 1\big) \Longleftrightarrow d = \text{pgcd}(a,b)$
3. Lemme d'Euclide

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

4. Lemme de Gauss

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

5. $(a|c,\ b|c \quad \text{et} \quad a \wedge b = 1) \Longrightarrow ab|c$
6. $ab = \text{pgcd}(a,b)\text{ppcm}(a,b)$

5. Nombres premiers et TFA

Définition (nombres premiers)

$n \in \mathbb{N}$ est dit premier (ou irréductible) si :

1. $n \neq 1$
2. $n = ab \Longrightarrow (a = 1 \text{ ou } b = 1)$

On désigne par $\mathbb{P}$ l'ensemble des nombres premiers.

Théorème (TFA)

Tout entier $n \neq 0$ s'écrit de manière unique

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

où $v_p(n) \in \mathbb{N}$ s'appelle valuation p-adique de n.

Démonstration : en TD ... □