Chapitre I
L'arithmétique, c'est fantastique !

Emmanuel Hallouin

L3 MIASHS, parcours Informatique-SHS, UT2J

Année 2021-2022

Les entiers naturels & relatifs

- L'ensemble des entiers *naturels*, noté $\mathbb{N}$, est :

$$\mathbb{N} = \{0, 1, 2, 3, 4, \ldots\}.$$

- L'ensemble des entiers *relatifs*, noté $\mathbb{Z}$, est :

$$\mathbb{Z} = \{\ldots, -4, -3, -2, -1\} \cup \{0, 1, 2, 3, 4, \ldots\}.$$

- Ils sont munis de deux lois :
  - la somme $+$, d'élément neutre 0 ($x + 0 = 0 + x = x$),
  - et le produit $\times$, d'élément neutre 1 ($x \times 1 = 1 \times x = x$).
- Dans $\mathbb{Z}$, tout élément x possède un *opposé* $-x$, vérifiant $x + (-x) = 0$.
- Dans $\mathbb{Z}$, un élément x ne possède pas forcément d'*inverse* $1/x$, vérifiant $x \times (1/x) = 1$.

Relation de divisibilité

Définition

Soit $a, b \in \mathbb{Z}$, On dit que a **divise** b ou que a est un **diviseur** de b ou que b est un **multiple** de a, s'il existe $q \in \mathbb{Z}$ tel que $b = a \times q$. On note $a \mid b$.

Exemples & Comportements particuliers

- $3 \mid 12$ car $12 = 3 \times 4$. $12 \nmid 3$ car $12 > 3$.
- L'entier 0 est divisible par n'importe quel entier (car $0 = 0 \times x$), mais il ne divise que lui même.
- Les entiers ± 1 divisent tous les entiers (car $x = 1 \times x$), mais ne sont divisibles par aucun entier autre qu'eux-mêmes.

Division euclidienne

Division euclidienne

Soit $a, b \in \mathbb{Z}$ avec a **non nul**. Alors il existe un unique couple $(q, r) \in \mathbb{Z}^2$ tel que :

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

où $|a|$ désigne la valeur absolue de a, $|a| = a$, si $a \geqslant 0$ et $-a$ si $a < 0$.

- L'entier q s'appelle le **quotient** de la division de b par a ;
- l'entier r s'appelle le **reste** de la division de b par a.

Exemples

- La division euclidienne et 11 par 5 : $11 = 5 \times 2 + 1$.

Caractérisation de la divisibilité

Soit a, b deux entiers. Alors a divise b si et seulement si le reste de la division euclidienne de b par a est nul.

pgcd et ppcm

Définition

- Le pgcd(a, b) c'est le plus grand diviseur commun entre a et b.
- Le ppcm(a, b) c'est le plus petit multiple commun positif entre a et b.

Exemples

- pgcd$(14, 21) = 7$ car $14 = 7 \times 2$ et $21 = 7 \times 3$.
- pgcd$(15, 26) = 1$.
- ppcm$(14, 21) = 2 \times 3 \times 7 = 42$.
- ppcm$(15, 26) = 15 \times 26$.

Relation «être premiers entre eux»

Définition

Soit a et b deux entiers. Ils sont dits premiers entre eux si et seulement si $\text{pgcd}(a, b) = 1$.

Cela veut dire que a et b ne sont tous les deux divisibles par aucun entier autres que ± 1.

Théorème de Bezout

Deux entiers a et b sont premiers entre eux si et seulement s'il existe $u, v \in \mathbb{Z}$ tels que $au + bv = 1$.

Les coefficients u, v du théorème précédent s'appellent des **coefficients de Bezout** ; ils ne sont pas uniquement définis. Leur existence découle de l'algorithme d'Euclide «étendu» (cf. la suite).

Algorithme d'Euclide

- **Entrée :** Deux entiers $a, b \in \mathbb{Z}$.
- Initialisation : $r_0 = a$, $r_1 = b$
- On divise $r_0 = a$ par $r_1 = b$, pour obtenir le reste r_2 ($|r_1| > r_2$).
- On recommence en divisant r_1 par r_2, pour obtenir le reste r_3 ($|r_1| > r_2 > r_3$).
- $\vdots$
- On itère jusqu'à trouver un reste nul, ce qui déclenche la fin de l'algorithme.
- **Sortie :** On retourne le dernier reste non nul ; c'est le pgcd(a, b).

Un exemple d'Algorithme d'Euclide

i	r_i	q_i	les divisions euclidiennes
0	163		
1	91		
2	72	1	$163 = 91 \times 1 + 72$
3	19	1	$91 = 72 \times 1 + 19$
4	15	3	$72 = 19 \times 3 + 15$
5	4	1	$19 = 15 \times 1 + 4$
6	3	3	$15 = 4 \times 3 + 3$
7	1	1	$4 = 3 \times 1 + 1$
8	0	3	$3 = 1 \times 3 + 0$

Le 8-ème reste est nul, le 7-ème ne l'est pas ; ce dernier est donc le pgcd . Ici $\text{pgcd}(163, 91) = 1$.

Les formules pour l'algorithme d'Euclide étendu

La suite des restes $(r_i)_{i\geqslant 0}$ est accompagnée du calcul d'une suite de couples $(u_i, v_i)_{i\geqslant 0}$ tels que $r_i = au_i + bv_i$.

- Données initiales :

$$\begin{array}{lll} r_0 = a & u_0 = 1 & v_0 = 0 \\ r_1 = b & u_1 = 0 & v_1 = 1 \end{array}$$

- Itération pour $i \geqslant 2$:

$$\begin{cases} (r_i, q_i) = & (\text{reste}, \text{quotient}) \text{ de la division} \\ & \text{euclidienne de } r_{i-2} \text{ par } r_{i-1} \\ u_i = u_{i-2} - q_i u_{i-1} \\ v_i = v_{i-2} - q_i v_{i-1} \end{cases}$$

L'exemple précédent dans sa version «étendue»

i	r_i	q_i	u_i	v_i	Les calculs pour les u_i, v_i
0	163		1	0	
1	91		0	1	
2	72	1	1	-1	$u_2 = u_0 - u_1 q_2 = 1 - 0 \times 1 = 1$ $v_2 = v_0 - v_1 q_2 = 0 - 1 \times 1 = -1$
3	19	1	-1	2	$u_3 = u_1 - u_2 q_3$ $v_3 = v_1 - v_2 q_3$
4	15	3	4	-7	
5	4	1	-5	9	
6	3	3	19	-34	
7	1	1	-24	43	
8	0	3	91	-163	

Ainsi : $\text{pgcd}(163, 91) = 1 = 162 \times (-24) + 91 \times 43$.

Notion d'entier «premier»

Définition

Un entier $p \in \mathbb{Z}$ est dit **premier** s'il n'est divisible que par exactement deux entiers 1 et lui même (au signe près).

Un nombre premier est un entier que l'on ne peut pas écrire comme le produit (non trivial) de deux entiers.
Exemples et contre-exemples

- 0 et 1 ne sont pas premiers.
- $2, 3, 5, 7, 11, 13, 17, 19, 23$ sont premiers.
- $8 = 2^3$ n'est pas premier.

Théorème

Il existe une infinité de premiers.

Théorème fondamental de l'arithmétique

Théorème

Tout entier est produit de nombres premiers et ce produit est unique à l'ordre près. Plus précisément, pour tout entier $n \in \mathbb{Z}$ il existe $p_1, \ldots, p_r$ des premiers et $e_1, \ldots, e_r$ des exposants tels que :

$$n = \pm p_1^{e_1} \times \cdots \times p_r^{e_r}.$$

Exemples :

- $8 = 2^3$
- $6 = 2^1 \times 3^1$
- $12 = 2^2 \times 3^1$

Th. fondamental et divisibilité

Soit a et $b \in \mathbb{Z}$ deux entiers décomposés en premiers :

$$a = p_1^{e_1} \times \cdots \times p_r^{e_r}, \qquad b = p_1^{f_1} \times \cdots \times p_r^{f_r}.$$

où les e_i, f_i sont $\geqslant 0$ (éventuellement nuls). Alors on a :

- $a \mid b$ si et seulement si $e_i \leqslant f_i$ pour tout i.
- et les formules :

$$\begin{aligned} \operatorname{pgcd}(a,b) &= p_1^{\min\{e_1,f_1\}} \times \cdots \times p_r^{\min\{e_r,f_r\}}, \\ \operatorname{ppcm}(a,b) &= p_1^{\max\{e_1,f_1\}} \times \cdots \times p_r^{\max\{e_r,f_r\}}. \end{aligned}$$

Taille d'un entier

La taille d'un entier n, c'est le nombre de bits de son écriture en base 2. L'ordre de grandeur de cette taille, c'est $\log(n)$. Plus précisément, la taille, est ce que l'on appelle un «grand O de $\log(n)$», noté $O(\log(n))$, c'est-à-dire un quantité inférieure à une certaine constante fois $\log(n)$.

- La taille d'une somme $a + b$, c'est un $O(\max\{\log(a), \log(b)\})$.
- La taille d'un produit $a \times b$, c'est un $O(\log(a) + \log(b))$.

Hiérarchie pour l'efficacité des algorithmes

Algorithmes sur $\mathbb{Z}$

Un algorithme prenant en entrée des entiers $\leqslant n$ est dit :

- **linéaire** s'il requiert un nombre d'opérations bit-à-bit en $O(\log(n))$.
- **quadratique** s'il requiert un nombre d'opérations bit-à-bit en $O(\log(n)^2)$.
- **cubique** s'il requiert un nombre d'opérations bit-à-bit en $O(\log(n)^3)$.
- **polynomial** s'il requiert un nombre d'opérations bit-à-bit en $O(\log(n)^k)$ pour un $k \in \mathbb{N}^*$.
- **exponentiel** s'il requiert un nombre d'opérations bit-à-bit en $O(n)$.

Algorithmes efficaces/inefficaces

Convention

La classe des algorithmes dits «efficaces» sont les algorithmes de complexité polynomiale.
Je dirai qu'un problème n'est pas résoluble efficacement, ou que le problème est difficile, si on ne connaît pas d'algorithme polynomial le résolvant.

Exemples.

- Les opérations élémentaires entre entiers sont **efficaces** (cf. diapo suivante).
- On ne connaît pas, à l'heure actuelle, d'algorithme polynomial permettant de factoriser un entier.

Efficacité des opérations élémentaires

Soit a, b deux entiers $\leqslant n$. Les complexités des opérations élémentaires sont les suivantes

Opération	Complexité en fonction de a et b	Complexité en fonction de n
$a + b$	$O(\log a + \log b)$	$O(\log n)$
$a - b$	$O(\log a + \log b)$	$O(\log n)$
$a \times b$	$O(\log a \log b)$	$O(\log^2 n)$
$a \div b$	$O((\log a - \log b) \log b)$	$O(\log^2 n)$
$\text{pgcd}(a, b)$	$O(\log a \log b)$	$O(\log^2 n)$

Remarque : pour ce qui concerne le produit, il existe des algorithmes meilleurs que les quadratiques (sans pour autant être linéaires).