Chapitre 12 : Rudiment d'arithmétique dans $\mathbb{N}$

I) Nombres entiers, décimaux, rationnels…

Définition : Voici des sous-ensembles de $\mathbb{R}$ que l'on utilise usuellement :

- $\mathbb{N}$ l'ensemble des entiers naturels : $\mathbb{N} = \{0; 1; 2; \dots\}$
- $\mathbb{Z}$ l'ensemble des entiers : $\mathbb{Z} = \{\dots; -2; -1; 0; 1; 2; \dots\} = \mathbb{N} \cup \mathbb{N}^-$
- $\mathbb{D}$ l'ensemble des nombres décimaux :

$$\mathbb{D} = \left\{\frac{a}{10^n}; a \in \mathbb{Z}, n \in \mathbb{N}\right\}$$

- $\mathbb{Q}$ l'ensemble des nombres rationnels :

$$\mathbb{Q} = \left\{\frac{a}{b}; a \in \mathbb{Z}, b \in \mathbb{N}^*\right\}$$

Propriété I.1 : On a les inclusions strictes suivantes :

$$\mathbb{N} \subsetneq \mathbb{Z} \subsetneq \mathbb{D} \subsetneq \mathbb{Q} \subsetneq \mathbb{R}$$

Dans ce chapitre nous allons nous intéresser presque exclusivement à $\mathbb{Z}$.

II) Diviseurs et multiples dans $\mathbb{Z}$

a) Généralité

Définition : Soient $(a, b) \in \mathbb{Z}^2, a \neq 0$. Dire que a divise b c´est dire qu´il existe $k \in \mathbb{Z}$ tel que : $a \times k = b$
On dit aussi que **a est un diviseur de b** ou que **b est un multiple de a**.
On note a|b.

Exemple II.a.1 : Trouver tous les diviseurs de 153.

Application II.a2 : Démontrer que pour tout $n \in \mathbb{Z}\backslash\{1\}$, *n-1 divise* $n^2 + 3n - 4$.

Application II.a.3 : Déterminer tous les couples d´entiers relatifs x et y tel que : $x^2 - y^2 = 11$

Propriété II.a.4 :

- 0 est multiple de tout entier de tout entier
- 1 est diviseur de tout entier

Propriété II.a.5 : Si a divise b et a divise c, alors a divise toute combinaison linéaire de b et c.
Ainsi pour tout entier relatif u et v, a divise *bu+cv*.

Application II.a.6 : Montrer que si a divise *3n-5* et a divise *2n+3*, alors a divise 19.

b) Division euclidienne

Propriété II.b.1 : Soit a un entier naturel et b un entier naturel non nul. Alors il existe un unique couple (q,r) tel que : $a = bq + r$ et $0 \leq r < b$.

Exemple II.b.2 : Déterminer la division euclidienne de 27 par 7.

Application II.b.3 : Ecrire une fonction Python pour déterminer q et r, respectivement quotient et reste dans la division euclidienne de a par b.

Propriété II.b.4 : Pour tout entier naturel n, on peut écrire :

- $n = 2k$ *ou* $n = 2k + 1$
- $n = 3k$ *ou* $n = 3k + 1$ *ou* $n = 3k + 2$
- $n = 4k$ *ou* $n = 4k + 1$ *ou* $n = 4k + 2$ *ou* $n = 4k + 3$

Application II.b.5 : Démontrer que pour tout entier naturel non nul, 3 divise $A_n = n(n^2 + 5)$

Remarque : Si deux entiers a *et* b ont le même reste dans la division euclidienne par c, on note alors : $a \equiv b[c]$

III) Diviseur et multiple commun

a) PGCD

Notation pratique : Soit a un entier non nul. Dans toute la suite on notera $\mathcal{D}_a^+$ l´ensemble des diviseurs positifs de a.

Exemple III.a.1 : Déterminer $\mathcal{D}_{24}^+$

Définition : Soit a et b deux entiers naturels non nul. L´ensemble des diviseurs commun de a et b admet un plus grand élément, appelé le PGCD de a et de b, noté PGCD(a ;b) ou a∧b.

Exemple III.a.2: Déterminer $24 \wedge 18$.

Remarque : Soit $(a; b) \in \mathbb{N}^2$. On a :

- $a \wedge b = b \wedge a$
- Si $a > 0, a \wedge 0 = a$
- Par convention $0 \wedge 0 = 0$

Extension de la définition : Si $(a; b) \in \mathbb{Z}^2$, on peut poser : $a \wedge b = |a| \wedge |b|$

b) Algorithme d´Euclide

Propriété III.b.1 (Lemme d´Euclide) : Soient a et b deux entiers naturels non nuls. On pose la division euclidienne de a par b : $a = bq + r$. Alors on a :

$$a \wedge b = b \wedge r$$

Conséquence (algorithme d´Euclide) : Pour déterminer le PGCD de deux nombres entiers, on peut utiliser l´algorithme d´Euclide (vu en troisième) :

Théorème 1 : Soit a et b deux naturels non nuls tels que b ne divise pas a.

La suite des divisions euclidiennes suivantes finit par s'arrêter. Le dernier reste non nul est alors le $\text{pgcd}(a, b)$

$$\begin{array}{rll}
a \text{ par } b & a = b\,q_0 + r_0 & \text{avec} \quad b > r_0 \geqslant 0 \\
b \text{ par } r_0 & b = r_0\,q_1 + r_1 & \text{avec} \quad r_0 > r_1 \geqslant 0 \\
r_0 \text{ par } r_1 & r_0 = r_1\,q_2 + r_2 & \text{avec} \quad r_1 > r_2 \geqslant 0 \\
\vdots & \vdots & \\
r_{n-2} \text{ par } r_{n-1} & r_{n-2} = r_{n-1}\,q_n + r_n & \text{avec} \quad r_{n-1} > r_n \geqslant 0 \\
r_{n-1} \text{ par } r_n & r_{n-1} = r_n\,q_{n-1} + 0 &
\end{array}$$

On a alors $\text{pgcd}(a, b) = r_n$.

***Application III.b.2* :** Déterminer $1071 \wedge 1029$

Application III.b.3 : Démontrer que deux entiers non nuls consécutifs ont un PGCD de 1.

c) Propriété du PGCD

Propriété III.c.1 : On a :

$$\forall\,(k,a,b)\in\mathbb{N}\times\mathbb{Z}^2,(ka\wedge kb)=k(a\wedge b)$$

Propriété III.c.2 : Soit $(a,b,d)\in\mathbb{N}^3$. On a :

$$d=a\wedge b\Leftrightarrow\begin{cases}d|a\\d|b\\\forall\,n\in\mathbb{N},(n|a\ et\ n|b)\Longrightarrow n|d\end{cases}$$

Propriété III.c.3 ***(Caractérisation du PGCD)*** : Soit $(a,b,d)\in\mathbb{N}^3$Soit d=PGCD(a ;b).

$$d=a\wedge b\Leftrightarrow\exists(a';b')\in\mathbb{N}^2,\begin{cases}a=da'\\b=db'\\PGCD(a';b')=1\end{cases}$$

Application III.c.4 : Résoudre :

$$\begin{cases}ab=2880\\PGCD(a;b)=12\end{cases}$$

d) PPCM

Définition : Soit a et b deux entiers naturels non nul. L´ensemble des multiples commun de a et b admet un plus petit élément, appelé le PPCM de a et de b, noté PPCM(a ;b) ou a∨b.

Exemple III.d.1 : Déterminer $24\vee 18$.

Remarque : Soit $(a;b)\in\mathbb{N}^2$. On a :

- $a\vee b=b\vee a$
- $a\vee 0=0$
- *Si a>0,* $a\wedge 1=a$

Propriété III.d.2 ***(Caractérisation du PPCM)*** : Soit $(a,b,n)\in(\mathbb{N}^*)^3$. On a :

$$m=a\vee b\Leftrightarrow\begin{cases}a|m\\b|m\\\forall\,m'\in\mathbb{N},(a|m'et\ b|m')\Longrightarrow m|m'\end{cases}$$

Propriété III.d.3 : On a :

$$\forall\,(a,b)\in\mathbb{N}^2,(a\vee b)\times(a\wedge b)=a\times b$$

IV) Nombres premiers

a) Bien connu

Définition : Soit p un nombre entier naturel. On dit que p est premier s´il admet exactement deux diviseurs : 1 et lui-même.

Exemple IV.a.1 : Déterminer les 5 premiers nombres premiers.

ATTENTION : 1 n´est pas premier.
Notation : Dans toute la suite de ce chapitre, on notera $\mathcal{P}$ l´ensemble des nombres premiers.

Propriété IV.a.2 : Soit n un nombre entier naturel strictement supérieur à 1. Alors soit n est premier, soit il existe un nombre premier p tel que p soit le plus petit diviseur positif (autre que 1) de n et $2 \leq p \leq \sqrt{n}$.

Application IV.a.3 : Démontrer que 109 est premier.

b) Infinitude

Définition : Le crible d'Ératosthène est un procédé qui permet de trouver tous les nombres premiers inférieurs à un certain entier naturel donné N.
L'algorithme procède par élimination : il s'agit de supprimer d'une table des entiers de 2 à N tous les multiples d'un entier. En supprimant tous les multiples, à la fin il ne restera que les entiers qui ne sont multiples d'aucun entier, et qui sont donc les nombres premiers.

Remarque : Le crible d´Eratosthène nous permet de déterminer les nombres premiers plus petit qu´un entier n. Cependant cet algorithme n´est pas du tout efficace pour des nombres très grands.

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

Propriété IV.b.1 : L´ensemble des nombres premiers est infini.

c) Théorème fondamentale de l´arithmétique

Propriété IV.c.1 (Théorème fondamentale) : Tout entier naturel n≥2 peut se décomposer de façon unique (à l´ordre des facteurs près), en produit de facteur premier :

$$n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$$

Exemple IV.c.2 : Décomposer 8465 en produit de facteur premier

Propriété IV.c.3 (PGCD ET PPCM) : Soit $(a; b) \in \mathbb{N}^2$. On pose leur décomposition en facteur premier :

$$a = \prod_{p \in \mathcal{P}} p^{\alpha_p} \quad et \quad b = \prod_{p \in \mathcal{P}} p^{\beta_p}$$

On a alors :

(1): $a|b \iff \forall p \in \mathcal{P}, \alpha_p \leq \beta_p$

(2): $a \wedge b = \prod_{p \in \mathcal{P}} p^{min(\alpha_p;\beta_p)}$

(3): $a \vee b = \prod_{p \in \mathcal{P}} p^{max(\alpha_p;\beta_p)}$

Exemple IV.c.4 : Déterminer $\mathcal{D}_{432}^{+}$

Application IV.c.5 : Déterminer $9100 \wedge 1848$ *et* $9100 \vee 1848$