Éléments d'arithmétique dans $\mathbb{N}$

Ce petit exposé d'arithmétique sera suivi d'un cours plus ambitieux : *Arithmétique dans* $\mathbb{Z}$.

On va d'ores et déjà expliquer que tout entier naturel supérieur à 2 se décompose comme un produit de nombres premiers, mais nous attendrons le *vrai* cours d'arithmétique pour énoncer le théorème fondamental de l'arithmétique, qui à l'existence de cette décomposition ajoute l'unicité, à l'ordre des facteurs près.

1 Divisibilité dans $\mathbb{N}$.

1.1 Définition.

Définition 1.

Soit $(a,b) \in \mathbb{N}^2$. On dit que b **divise** a (on note $b \mid a$) s'il existe un entier $k \in \mathbb{N}$ tel que $a = kb$.
Si $b \mid a$, on dit encore que b est un **diviseur** de a ou que a est un **multiple** de b.

Pour un entier naturel a, on notera $\mathcal{D}(a)$ l'ensemble des diviseurs de a.

Exemple 2.

1. 1, 2, 3, 4, 6 et 12 sont les diviseurs de 12 : $\mathcal{D}(12) = \{1,2,3,4,6,12\}$.
2. 1 divise tout nombre entier.
3. Tous les entiers sont diviseurs de 0 : $\mathcal{D}(0) = \mathbb{N}$. Zéro ne divise que lui-même.
4. Pour tout entier naturel n, $4^n - 1$ est un multiple de 3.

Proposition 3.

Dans $\mathbb{N}$, les diviseurs d'un entier naturel a non nul sont compris entre 1 et a.

Proposition 4.

La relation $\mid$ (divise) est une relation d'ordre sur $\mathbb{N}$ (ordre non total). Plus précisément

1. $\forall a \in \mathbb{N}\ a \mid a$ (réflexivité)
2. $\forall (a,b) \in \mathbb{N}^2\ (a \mid b \text{ et } b \mid a) \implies a = b$ (antisymétrie)
3. $\forall (a,b,c) \in \mathbb{N}^3\ (a \mid b \text{ et } b \mid c) \implies a \mid c$ (transitivité)

1.2 Division euclidienne.

Voici deux « divisions » de 22 par 4 dans $\mathbb{N}$: $\begin{cases} 22 &= 4\times 4+6 \\ 22 &= 4\times 5+2 \end{cases}$
Il n'y a rien à redire à la première égalité sinon que l'on peut encore trouver une fois 4 dans le reste 6. La seconde division est de ce point de vue meilleure : ce sera la division euclidienne de 22 par 4.

Théorème 5.

Soit $(a,b)\in\mathbb{N}\times\mathbb{N}^*$. Il existe un unique couple $(q,r)\in\mathbb{N}^2$ tel que

$$a=bq+r \quad \text{et} \quad 0\leq r<b.$$

Les entiers q et r sont appelés respectivement **quotient** et **reste** dans la division euclidienne de a par b.

Exemple. On pose la division de 666999 par 123, en utilisant la méthode apprise à l'école primaire.

Proposition 6.

Soit a et b deux entiers (b non nul).
L'entier b divise a si et seulement le reste dans la division euclidienne de a par b est nul.

1.3 Diviseurs communs à deux entiers naturels.

Lemme 7.

Soit $(a,b)\in\mathbb{N}^2\setminus\{(0,0)\}$ (a et b sont deux entiers naturels *dont l'un au moins est non nul*).
Alors $\mathcal{D}(a)\cap\mathcal{D}(b)$, ensemble des diviseurs communs à a et b contient 1 et est majoré par $\max(a,b)$.

Définition 8.

Soit $(a,b)\in\mathbb{N}^2\setminus\{(0,0)\}$. On appelle **Plus Grand Commun Diviseur** (PGCD) de a et b, et on note $a\wedge b$ (ou $\text{PGCD}(a,b)$) le plus grand diviseur commun à a et b pour la relation $\leq$:

$$a\wedge b=\max\left(\mathcal{D}(a)\cap\mathcal{D}(b)\right).$$

Lemme 9.

Soit $(a,b,c,q)\in\mathbb{N}^4$ tel que $a=bq+c$. Alors $\mathcal{D}(a)\cap\mathcal{D}(b)=\mathcal{D}(b)\cap\mathcal{D}(c)$,

Proposition 10.

$$\forall(a,b)\in\mathbb{N}^2\setminus\{(0,0)\} \qquad \mathcal{D}(a)\cap\mathcal{D}(b)=\mathcal{D}(a\wedge b).$$

Preuve. Quitte à échanger a et b, on peut supposer que b est non nul.

• Posons $r_{-1} = a$ et $r_0 = b$.

• Par itération, on va définir une suite $q_1, \dots q_{p+1}$ et $r_1, \dots, r_{p+1}$ de la manière suivante : pour $n \in \mathbb{N}$, si r_n est non nul, on effectue la division euclidienne de r_{n-1} par r_n en notant q_{n+1} et r_{n+1} respectivement son quotient et son reste. Ainsi, si $r_n \neq 0$, on a $r_{n+1} < r_n$. La suite (r_n) est donc suite d'entiers strictement décroissante puis stationnaire à 0. Notons p le rang de son dernier terme non nul.

$$\begin{aligned} a &= b \cdot q_1 + r_1 \\ r_0 &= r_1 \cdot q_2 + r_2 \\ r_1 &= r_2 \cdot q_3 + r_3 \\ &\dots \\ r_{p-2} &= r_{p-1} \cdot q_p + r_p \\ r_{p-1} &= r_p \cdot q_{p+1} + 0 \end{aligned}$$

D'après le lemme précédent, on a les égalités suivantes entre ensembles de diviseurs :

$$\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(r_0) \cap \mathcal{D}(r_1) = \mathcal{D}(r_1) \cap \mathcal{D}(r_2) = \dots = \mathcal{D}(r_{p-1}) \cap \mathcal{D}(r_p) = \mathcal{D}(r_p) \cap \underbrace{\mathcal{D}(0)}_{=\mathbb{N}} = \mathcal{D}(r_p).$$

$$r_p = \max\left(\mathcal{D}(r_p)\right) = \max\left(\mathcal{D}(a) \cap \mathcal{D}(b)\right) = a \wedge b.$$

□

On apprend dans la preuve ci-dessus un algorithme de calcul du PGCD, appelé **algorithme d'Euclide**.

Algorithme 11 (Algorithme d'Euclide (écrit en Python)).

```
def PGCD(a,b):
    while b!=0:
        a,b=b,a%b    # a%b : reste dans la div.eucl. de a par b
    return a
```

Exemple 12.

Calculer le PGCD de 342 et 95 puis donner $\mathcal{D}(342) \cap \mathcal{D}(95)$.

Remarque. Pour a et b deux entiers naturels non tous les deux nuls, on a

1. $a \wedge b \in \mathcal{D}(a) \cap \mathcal{D}(b)$
   i.e. $a \wedge b$ est un diviseur commun de a et b.
2. $\forall \delta \in \mathcal{D}(a) \cap \mathcal{D}(b) \quad \delta \in \mathcal{D}(a \wedge b)$
   i.e. $a \wedge b$ est le plus grand des diviseurs communs au sens de la relation d'ordre divise.

2 Nombres premiers.

Définition 13.

Un entier $p \in \mathbb{N} \setminus \{0,1\}$ est dit **premier** si ses seuls diviseurs sont 1 et p.

Exemples. 2, 3, 5, 7, 11, 13...

Proposition 14.

Tout entier naturel supérieur ou égal à 2 admet un diviseur premier.

On peut affiner « quantitativement » le résultat précédent.

Proposition 15.

Pour tout entier naturel n non premier et supérieur à 2 admet un diviseur premier inférieur à $\sqrt{n}$.

Application : crible d'Eratosthène. Un nombre *non* premier inférieur à 100 a d'après ce qui précède un diviseur premier inférieur à 10. Ainsi, une fois éliminés de la grille ci-dessous tous les multiples (non triviaux) de 2, 3, 5 et 7, il ne restera que les entiers premiers inférieurs à 100.

0	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

Théorème 16 (d'Euclide).

Il existe une infinité de nombres premiers.

Proposition 17 (Existence d'une décomposition en facteurs premiers).

Pour tout entier $n \geq 2$, il existe un entier $r \geq 1$, des nombres premiers $p_1, p_2, \dots p_r$, et des entiers non nuls $\alpha_1, \dots \alpha_r$ tels que

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdot p_r^{\alpha_r}.$$

Exemple. Décomposer 36 milliards en produit de facteurs premiers.