Chapitre 19

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

Sommaire.

1 Divisibilité dans $\mathbb{N}$. **1**
1.1 Définition. 1
1.2 Division euclidienne. 1
1.3 Diviseurs communs à deux entiers naturels. 2

2 Nombres premiers **2**

Les propositions marquées de ★ sont au programme de colles.

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 exisite $k \in \mathbb{N}$ 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.
2. 1 divise tout nombre entier : $\forall n \in \mathbb{N},\ n = 1n$.
3. Tous les entiers sont diviseurs de 0 : $\forall n \in \mathbb{Z},\ 0/n = 0$.
4. Pour tout entier naturel n, $4^n - 1$ est multple de 3 : $4^n - 1 = 3\sum_{k=0}^{n-1} 4^k$.

Proposition 3

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

Preuve :

Soit $a \in \mathbb{N}^*$ et $b \in \mathcal{D}(a)$: $\exists k \in \mathbb{N} \mid a = kb$.
Si $b = 0$, alors $a = 0$: impossible donc $b \geq 1$.
Si $b > a$, alors $kb > a$ donc $a > a$: impossible donc $b \leq a$.

Proposition 4

La relation $\mid$ est une relation d'ordre non total sur $\mathbb{N}$.

1.2 Division euclidienne.

Théorème 5

Soit $(a,b) \in \mathbb{N} \times \mathbb{N}^*$.

$$\exists!(q,r) \in \mathbb{N}^2 \mid a = bq + r \quad \text{et} \quad 0 \leq r < b.$$

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

Preuve :

Unicité. Soient $(q,r) \in \mathbb{N}^2$ et $(q',r') \in \mathbb{N}^2$ tels que $a = bq + r = bq' + r'$ et $r, r' < b$.
Alors $b(q-q') + (r-r') = 0$, or $-b < r' - r < b$ donc $-b < b(q-q') < b$ donc $-1 < q - q' < 1$ donc $q = q'$.
Alors $r - r' = 0$ donc $r = r'$: $(q,r) = (q',r')$.

Existence. Posons $q = \left\lfloor \frac{a}{b} \right\rfloor$ et $r = a - bq$. On a:

$$\begin{aligned} \left\lfloor \frac{a}{b} \right\rfloor \leq \frac{a}{b} < \left\lfloor \frac{a}{b} \right\rfloor + 1 \quad & \text{donc} \quad q \leq \frac{a}{b} < q + 1 \\ & \text{donc} \quad bq \leq a < bq + b \\ & \text{donc} \quad 0 \leq a - bq < b \end{aligned}$$

Donc $r \in [0, b[$ et $a = bq + r$.

Proposition 6

Soient $(a,b) \in \mathbb{N} \times \mathbb{N}^*$.
$$b \mid a \iff \exists! q \in \mathbb{N} \mid a = bq.$$

1.3 Diviseurs communs à deux entiers naturels.

Définition 7

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

Preuve :

• $1 \in \mathcal{D}(a)$ et $1 \in \mathcal{D}(b)$ donc $1 \in \mathcal{D}(a) \cap \mathcal{D}(b)$.
• Si $a \neq 0$ et $b \neq 0$, alors $\mathcal{D}(a) \subset [\![1, a]\!]$ et $\mathcal{D}(b) \subset [\![1, b]\!]$. Alors $\mathcal{D}(a) \cap \mathcal{D}(b) \subset [\![1, \min(a,b)]\!]$.
• Si $a \neq 0$ et $b = 0$ SPDG, $\mathcal{D}(b) = \mathbb{N}$ donc $\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(a) \subset [\![1, a]\!]$.
Dans tous les cas, $\mathcal{D}(a) \cap \mathcal{D}(b)$ est majoré par $\max(a,b)$, c'est une partie de $\mathbb{N}$ non vide et majorée : le max existe.

Lemme 8

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

Preuve :

Soit $k \in \mathcal{D}(a) \cap \mathcal{D}(b)$: $\exists a', b' \in \mathbb{N} \mid a = ka',\ b = kb'$. Alors $ka' = kb'q + c$ et $c = k(a' - b'q)$.
• Si $k > 0$, alors puisque $c \geq 0$, $a' - b'q \geq 0$ donc $k \mid c$ et $k \mid b$.
• Si $k = 0$, alors $a = b = 0$ puis $c = 0$ donc $k \mid b$ et $k \mid c$.
On a bien $\mathcal{D}(a) \cap \mathcal{D}(b) \subset \mathcal{D}(b) \cap \mathcal{D}(c)$.

Soit $k \in \mathcal{D}(b) \cap \mathcal{D}(c)$: $\exists b', c' \in \mathbb{N} \mid b = kb'$ et $c = kc'$.
Alors $a = bq + c = k(b'q + c)$ donc $k \mid a$. On a $\mathcal{D}(b) \cap \mathcal{D}(c) \subset \mathcal{D}(a) \cap \mathcal{D}(b)$.

Alors $\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(b) \cap \mathcal{D}(c)$.

Proposition 9

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

Preuve :

On suppose que $b \neq 0$. On pose $r_{-1} = a$ et $r_0 = b$.
Par itération, on définit deux suites (q_n) et (r_n) telles que 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 strictement décroissante puis stationnaire à 0. Notons p le rang de son dernier terme non nul.
$$a = bq_1 + r_1; \qquad r_0 = r_1 q_2 + r_2; \quad \ldots \quad ; r_{p-1} = r_p q_{p+1} + 0.$$

D'après le lemme précédent, on a les égalités suivantes entre ensembles de diviseurs :
$$\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(r_0) \cap \mathcal{D}(r_1) = \mathcal{D}(r_1) \cap \mathcal{D}(r_2) = \ldots = \mathcal{D}(r_p) \cap \mathcal{D}(0) = \mathcal{D}(r_p).$$

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

Algorithme 10: Algorithme d'Euclide (écrit en Python)

```
def PGCD(a,b):
    while b!=0:
        a,b=b,a%b
    return a
```

Exemple 11

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

Solution :

$392 = 95 \times 3 + 57$; $95 = 57 \times 1 + 38$; $57 = 38 \times 1 + 19$; $38 = 19 \times 2 + 0$ donc $\mathrm{PGCD}(342, 95) = 19$.
$\mathcal{D}(342) \cap \mathcal{D}(95) = \mathcal{D}(19) = [\![1, 19]\!]$.

2 Nombres premiers

Définition 12

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...

Proposition 13

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

Preuve :

Pour $n \in \mathbb{N}$, on pose $\mathcal{P}(n)$: « n a un diviseur premier ».
Initialisation. $\mathcal{P}(2)$ est vraie car 2 est premier et $2 \mid 2$.
Hérédité. Soit $n \geq \in \mathbb{N} \mid \forall k \in [\![2, n]\!],\ \mathcal{P}(k)$.
• Si $n+1$ est premier, alors $n+1 \mid n+1$: $\mathcal{P}(n+1)$ vraie.
• Si n n'est pas premier, $\exists (q, q') \in [\![2, n]\!]^2 \mid n+1 = qq'$.
Alors q a un diviseur premier par hypothèse, ce diviseur divise aussi $n+1$ par transitivité : $\mathcal{P}(n+1)$ vraie.
Par récurrence, $\forall n \geq 2,\ \mathcal{P}(n)$ est vraie.

Proposition 14

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

Preuve :

Soit $n \geq 2$ non premier : $\exists (q, q') \in [\![2, n-1]\!]^2 \mid n = qq'$ donc $q \leq \sqrt{n}$ ou $q' \leq \sqrt{n}$.
En effet, si $q \geq \sqrt{n}$ et $q' \geq \sqrt{n}$, alors $qq' > n$: impossible.
SPDG, $q \leq \sqrt{n}$. Or $q \geq 2$ donc q a un diviseur premier p donc $p \leq q \leq \sqrt{n}$ et $p \mid n$.

Théorème 15: d'Euclide.

Il existe une infinité de nombres premiers.

Preuve :

Supposons qu'il en existe un nombre fini n de nombres premiers $p_1, p_2, ...p_n$.
On pose $N = 1 + \prod_{k=1}^{n} p_k$. Alors $\forall k \in [\![1, n]\!],\ N > p_k$, donc N admet un diviseur premier.
Ainsi, $\exists k_0 \in [\![1, n]\!]\ :\ p_{k_0} \mid N$ et $p_{k_0} \mid N-1$ donc $p_{k_0} \mid N - (N-1) = 1$, absurde.

Proposition 16: Existence d'une décomposition en facteurs premiers.

Pour tout entier $n \geq 2$, il existe un entier $r \geq 1$ et des nombres premiers $p_1, ..., p_r$ et des entiers non nuls $\alpha_1, ..., \alpha_r$ tels que
$$n = p_1^{\alpha_1} \times ... \times p_r^{\alpha_r}.$$

Proposition 17: Théorème de La Vallée Poussin-Hadamard.

Soit la fonction π qui à n associe le nombre de nombres premiers inférieurs ou égaux à n. Alors
$$\lim_{n \to +\infty} \frac{\pi(n) \ln(n)}{n} = 1.$$