Divisibilité, nombres premiers

Objectifs :

- Connaître et savoir utiliser la notion de divisibilité dans $\mathbb{Z}$
- Comprendre la définition d'un nombre premier, et savoir en utiliser quelques premières propriétés
- Savoir combiner les outils issus des notions précédentes pour modéliser puis résoudre des problèmes

Aperçu historique :

Dans ces premiers chapitres, nous allons nous initier à *l'arithmétique* (du grec arithmos - nombre), qui est la branche des mathématiques consacrée à l'étude des nombres, et plus particulièrement des entiers (naturels puis relatifs).
L'origine de l'arithmétique semble être une invention phénicienne (Liban actuel). Dans l'école pythagoricienne, à la deuxième moitié du VIe siècle av. J.-C., l'arithmétique était, avec la géométrie, l'astronomie et la musique, une des quatre sciences quantitatives ou mathématiques (Mathemata).
Quant aux nombres premiers, on en trouverait trace sur l'os d'Ishango daté à plus de 20 000 ans avant notre ère. Des tablettes d'argile séchées Mésopotamiennes (Irak actuel) du IIe millénaire av. J.-C. montrent la résolution de problèmes qui suggèrent l'utilisation de nombres premiers.
Dans les mathématiques égyptiennes, le calcul fractionnaire , qui ne considérait que les inverses d'entiers (1/2, 1/3, 1/4, 1/5, ...) nécessitait de disposer d'une liste de nombres premiers.
La première trace incontestable de la présentation des nombres premiers remonte à l'Antiquité (vers 300 av. J.-C.), et se trouve dans les Éléments d'Euclide (livres VII à IX). Euclide donne la définition des nombres premiers, la preuve de leur infinité, la définition du plus grand commun diviseur (pgcd) et du plus petit commun multiple (ppcm), et les algorithmes pour les déterminer, aujourd'hui appelés algorithmes d'Euclide. Les connaissances présentées lui sont toutefois bien antérieures.

Euclide

1. Divisibilité dans $\mathbb{Z}$

Définition 2.1 $\mathbb{Z}$ désigne l'ensemble des entiers relatifs, et $\mathbb{N}$ celui des entiers naturels.

$\mathbb{N}$ est inclus dans $\mathbb{Z}$. On note $\mathbb{N} \subset \mathbb{Z}$. Ainsi, le nombre -6 est non seulement dans $\mathbb{Z}$, mais aussi dans $\mathbb{N}$.

Définition 2.2 Soient a et b des entiers relatifs, avec $b \neq 0$.
On dit que b *divise* a et on note $b|a$ s'il existe un entier relatif k tel que $a = k \times b$.
On dit aussi que *b est un diviseur de a*, ou encore que *a est un multiple de b*.

Remarque 2.1 $a = k \times b \Leftrightarrow a = (-k) \times (-b)$, donc si $b|a$, alors $-b|a$. De la même manière, $a = k \times b \Leftrightarrow -a = (-k) \times b$, donc si $b|a$, alors $b|(-a)$. Chercher les diviseurs de a dans $\mathbb{Z}$ revient donc à chercher les diviseurs de $|a|$ dans $\mathbb{N}$.

Exemple 2.1 :
- 56 est un multiple de -8 car $56 = (-7) \times (-8)$
- L'ensemble des multiples de 5 est $\{...; -15; -10; -5; 0; 5; 10; 15; ...\}$, on le notera $5\mathbb{Z}$. C'est le même que l'ensemble des multiples de -5.

Propriété 2.1 Premières conséquences
- Tout entier relatif divise 0
- Les seuls diviseurs de -1 et 1 sont -1 et 1
- -1 et 1 divisent tous les entiers relatifs
- Pour tout $a \in \mathbb{Z}$, $-a$ et a divisent a
- deux entiers relatifs opposés ont les mêmes diviseurs

Propriété 2.2 Soient a, b, c trois entiers relatifs non nuls.
1. Si $a|b$ et $b|a$, alors a et b sont égaux ou opposés.
2. Si $c|b$ et $b|a$, alors $c|a$.
3. Si c divise a et b, alors pour tous entiers relatifs u et v, c divise $ua + bv$.

Démonstration :
- $a|b$, donc il existe $k \in \mathbb{Z}$ t.q. $b = ka$. De la même manière, $b|a$, donc il existe $k' \in \mathbb{Z}$ t.q. $a = k'b$. Par suite, $b = kk'b$, donc $kk' = 1$. Ainsi, $k = k' = 1$ ou $k = k' = -1$ (seuls diviseurs de 1), d'où le résultat annoncé.
- $c|b$, donc il existe $k \in \mathbb{Z}$ t.q. $b = kc$. De la même manière, $b|a$, donc il existe $k' \in \mathbb{Z}$ t.q. $a = k'b$. Ainsi, $a = k'b = k'kc = \ell c$, en notant $\ell = k'k$. On a bien $\ell \in \mathbb{Z}$, donc $c|a$.
- $c|a$, donc il existe $k \in \mathbb{Z}$ t.q. $a = kc$. De la même manière, $c|b$, donc il existe $k' \in \mathbb{Z}$ t.q. $b = k'c$. Soient deux entiers relatifs quelconques u et v, il vient $ua + bv = ukc + vk'c = (uk + vk')c$, avec $uk + vk' \in \mathbb{Z}$, donc $c|(ua + bv)$

Remarque 2.2 En particulier, pour u et v égaux à 1 ou -1, il vient :
si $c|a$ et $c|b$, alors $c|(a + b)$, $c|(a - b)$, et $c|(b - a)$.

2. Nombres premiers

Définition 2.3 Un entier naturel est ***premier*** si et seulement si il admet exactement deux diviseurs : 1 et lui-même. Un entier supérieur à 1 et non premier est dit ***composé***.

Ainsi 1 n'est pas premier, et 2 est le seul nombre premier pair.

Propriété 2.3 Soit n un entier supérieur ou égal à 2.
n est premier ssi n n'a pas de diviseur premier inférieur ou égal à $\sqrt{n}$.

Démonstration Démonstration faite en exercice.

Propriété 2.4 Soit n un entier supérieur ou égal à 2.
Alors n est premier ou n peut s'écrire comme produit de nombres premiers.

En particulier, tout entier supérieur ou égal à 2 admet au moins un diviseur premier.

Démonstration Démonstration faite en exercice.

Théorème 2.1 Théorème fondamental de l'arithmétique : décomposition en facteurs premiers Tout entier $n \geqslant 2$ s'écrit de manière unique (à l'ordre des facteurs près) sous la forme d'un produit de nombres premiers :

$$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times p_3^{\alpha_3} \times ..... \times p_m^{\alpha_m}$$

où $p_1, p_2, p_3, ..., p_m$ sont des nombres premiers tels que $p_1 < p_2 < p_3 < ... < p_m$
et les exposants $\alpha_1, \alpha_2, \alpha_3, ..., \alpha_m$ sont des entiers naturels non nuls.
Cette écriture est la **décomposition en facteurs premiers** du nombre n.

Démonstration La propriété 2.4 assure l'existence de cette décomposition.
Nous en démontrerons l'unicité en exercice, après avoir défini la notion de nombres premiers entre eux.

Méthode :
La méthode dite "de l'échelle" pour décomposer un entier en facteurs premiers **est présentée dans la vidéo** Youtube "Decomposition d'un entier en facteurs premiers", sur la chaîne Maths Langella, playlist "TermS".

Théorème 2.2 L'ensemble des nombres premiers est infini.

Démonstration :
On travaille dans $\mathbb{N}$.
Raisonnons **par l'absurde**, et supposons qu'il existe un nombre fini de nombres premiers.
Soit P le plus grand d'entre eux.
On pose $n = 2 \times 3 \times 5 \times 7... \times P + 1$, le produit de tous les nombres premiers, augmenté de 1.
Comme n est un entier, il admet, d'après la conséquence de la propriété 2.4, au moins un diviseur premier.
Soit q un diviseur premier de n.
Comme q est premier, c'est l'un des facteurs du produit $2 \times 3 \times 5 \times 7... \times P$, on a donc $q|2 \times 3 \times 5 \times 7... \times P$
Or $n = 2 \times 3 \times 5 \times 7... \times P + 1 \Rightarrow 2 \times 3 \times 5 \times 7... \times P = n - 1$.
Comme $q|2 \times 3 \times 5 \times 7... \times P$, on a $q|(n-1)$.
Finalement, $q|n$ et $q|(n-1)$, donc $q|n-(n-1)$, i.e. $q|1$, donc $q = 1$.
Cela contredit l'hypothèse "q premier", donc notre hypothèse "il existe un nombre fini de nombres premiers" est fausse, donc l'ensemble des nombres premiers est infini.
L'idée de cette démonstration est attribuée à Euclide (III siècle av. notre ère).