Divisibilité : cours

Définition 1. *Soit $a, b \in \mathbb{Z}$. On dit que a divise b (ou b est divisible par a, ou a est un diviseur de b, ou encore b est un multiple de a) et on écrit $a \mid b$, s'il existe $c \in \mathbb{Z}$ tel que $b = ac$.*

Voici quelques propriétés élémentaires de divisibilité (a, b, et c désignent des entiers).

1. $a \mid a$.
2. Si $a \mid b$, alors $a \mid -b$ et $-a \mid b$ (et donc $-a \mid -b$).
3. $1 \mid a$.
4. Si $a \mid 1$, alors soit $a = 1$ soit $a = -1$.
5. $a \mid 0$.
6. 0 ne divise rien.
7. Si $a \mid b$, alors $a \mid cb$.
8. Si $a \mid b$ et $b \mid c$ alors $a \mid c$.
9. Si $a \mid b$ et $a \mid c$ alors $a \mid b + c$ (et donc $a \mid b - c$).

Grâce à la propriéte 2. il suffit d'étudier la divisibilité des entiers naturels. Désormais, si le contraire n'est pas indiqué, tous les nombres qui interviennent sont des entiers naturels, et le mot "diviseur" va désigner les diviseurs naturels.

Définition 2. *On dit que p est un nombre premier s'il n'a pas d'autres diviseurs que 1 et p. Par convention 1 n'est pas un nombre premier.*

Les nombres premiers sont les "blocs élémentaires" qui permettent de "construire" tous les autres entiers au sens suivant.

Théorème 1 (Théorème fondamental de l'arithmétique)**.** *Pour tout $a \in \mathbb{N}$ il existe une unique (à l'ordre près) décomposition en produit de puissances de nombres premiers :*

$$a = p_1^{\alpha_1} \cdot \dots \cdot p_m^{\alpha_m},$$

où $p_1, \dots, p_m$ sont des nombres premiers distincts et $\alpha_1, \dots, \alpha_m$ sont des entiers positifs.

Montrons d'abord l'éxistence d'une telle décomposition. Cette démonstration est basée sur une propriété très importante de $\mathbb{N}$: dans tout sous-ensemble de $\mathbb{N}$ il existe un plus petit élément.

Premièrement nous avons besoin d'un lemme (un résultat auxilière).

Lemme 1. *Tout entier naturel $n \neq 1$ est divisible par au moins un nombre premier.*

Démonstration :

Si $n = 0$, c'est évident grâce à la propriété 5.

Si n est un nombre premier, alors il est divisible par lui même.

Supposons maintenant que n n'est pas premier. Alors, par définition, il a d'autres diviseurs que 1 et n. Soit d le plus petit parmi eux. Alors $n = dn_1$, $n_1 \neq 1$.

Si d n'est pas premier, alors il existe $d_1 \neq 1$ et $d_2 \neq 1$ tels que $d = d_1 d_2$. Donc $n = d_1 d_2 n_1$, donc d_1 est un diviseur de n. Or $d_1 < d$, car $d_2 \neq 11$, ce qui contredit la supposition que d est le plus petit diviseur de n. Ainsi d est un diviseur premier. CQFD

Maintenant, si n est un nombre premier, alors $n = n$ est une decomposition de la forme qu'on recherche.

Si n n'est pas premier, alors, d'apres le lemme, il admet au moins un diviseur premier. Notons p_1 le plus petit diviseur premier de n. Alors $n = p_1 n_1$, où $n_1 < n$.

Si n_1 est un premier différent de p_1, alors on a la décomposition recherchée.

Si $n_1 = p_1$, alors $n = p^2$ est une telle décomposition.

Si n_1 n'est pas un nombre premier, alors on peut répéter le procédé en prenant p_2 le plus petit diviseur premier de n_1. On obtient alors $n = p_1 n_1 = p_1 p_2 n_2$, où $n_2 < n_1 < n$. Et ainsi de suite.

Vu qu'il n'y a qu'un nombre fini d'entiers positifs strictement inférieurs à n, au bout d'un nombre fini d'itérations on obtient alors une décomposition $n = p_1 \cdot \cdots \cdot p_k$, où tous les termes sont des nombres premiers non necessairement distincts. Il reste à regrouper les termes égaux pour retrouver la décomposition recherchée.

Pour montrer l'unicité d'une telle décomposition nous avons besoin d'un autre lemme.

Lemme 2 (Lemme d'Euclide)**.** *Si un nombre premier p divise ab, alors il divise soit a, soit b, soit les deux.*

Démonstration.

Supposons qu'il existe un tel p premier et des tels a et b que $p \mid ab$ mais $p \nmid a$ et $p \nmid b$. On prend le plus petit p qui vérifie cette condition et pour ce p on prend a et b tels que ab soit le plus petit possible.

Tout d'abord, dans ce cas $a < p$ et $b < p$ (si p.ex. $a > p$, alors $p \mid (a-p)b = ab - pb$ et $(a-p)b < ab$).

Ensuite, comme $p \mid ab$, on peut écrire $ab = pc$. Alors

$$c = \frac{ab}{p} < \frac{p^2}{p} = p,$$

et donc le plus petit diviseur p_1 de c est un nombre premier plus petit que p et qui divise ab. Alors $p_1 \mid a$ ou $p_1 \mid b$ (ou les deux), car p est le plus petit nombre premier qui ne vérifie pas cette propriété.

Sans perte de généralité on peut supposer que $p_1 \mid a$. Donc on a $a = p_1 a_1$ et $c = p_1 c_1$. Alors

$$a_1 b = \frac{p_1 a_1 b}{p_1} = \frac{ab}{p_1} = \frac{pc}{p_1} = \frac{p p_1 c_1}{p_1} = p c_1.$$

Donc $p \mid a_1 b$, mais $p \nmid a_1$ (sinon $p \mid a$, car $a_1 \mid a$) et $p \nmid b$. Or $a_1 b < ab$ ce qui contredit la minimalité de ab.

Alors notre première hypothèse est fausse, et il n'existe pas de tels p, a et b. CQFD

On peut maintenant montrer l'unicité de notre décomposition. Prenons deux produits de nombres premiers qui sont égaux. Prenons n'importe quel nombre premier p du premier produit. Il divise le premier produit, et donc, aussi le second. Par le lemme d'Euclide, p doit alors diviser au moins un facteur dans le second produit. Mais les facteurs sont tous des nombres premiers eux-mêmes, donc p doit être égal à un des facteurs du second produit. Nous pouvons donc simplifier par p les deux produits. On repète le procédé sur les quotients. Au moment où on aura épuisé tous les facteurs premièrs du premièr produit (donc on aura obtenu le quotient 1), de l'autre côté il ne restera plus rien non plus, car les deux produits etaient égaux au départ.

Remarque 1. *Une fois qu'on a ce théorème, on peut dire que a divise b si et seulement si tout diviseur premier de a entre dans la décomposition de b avec une puissance au moins égale à celle avec laquelle il entre en décomposition de b. Par exemple $2^4 \cdot 3^5 \cdot 17$ divise $2^6 \cdot 3^{10} \cdot 17^2 \cdot 239$, mais $2^7 \cdot 17^2 \cdot 19 \cdot 239$ ne le divise pas.*

Définition 3. *On dit que deux entiers a et b sont premiers entre eux si leur seul diviseur commun est 1.*

Grâce au théorème précédent, dire que deux nombres entiers sont premiers entre eux revient à dire que dans leurs décompositions en produit de facteurs premiers il n'y a pas de termes communs.

Définition 4.
1. *On appelle le plus grand diviseur commun de a et b (et on note $pgcd(a,b)$, ou encore $a \vee b$) le plus grand nombre d tel que $d \mid a$ et $d \mid b$.*
2. *On appelle le plus petit multiple commun de a et b (et on note $ppcm(a,b)$) le plus petit nombre m tel que $a \mid m$ et $b \mid m$.*

Propriétés :

1. Si $d = pgcd(a,b)$ et d_1 est tel que $d_1 \mid a$ et $d_1 \mid b$, alors $d_1 \mid d$.
2. Si $m = ppcm(a,b)$ et m_1 est tel que $a \mid m_1$ et $b \mid m_1$, alors $m \mid m_1$.
3. Deux nombres a et b sont premiers entre eux si et seulement si $pgcd(a,b) = 1$.
4. Deux nombres a et b sont premiers entre eux si et seulement si $ppcm(a,b) = ab$.