Nombres Premiers

1 Nombres Premiers

Un **nombre premier** est un entier p qui est seulement divisible par ± 1 et $\pm p$, et qui est strictement plus grand de 1. Les nombres premiers sont donc les entiers naturels avec deux diviseurs positifs. On utilise la notation $\mathcal{P}$ pour l'ensemble des nombres premiers (qui est infini !) :

$$\mathcal{P} = \{2, 3, 5, 7, 11, 13, 17, 19, 23 \ldots\}.$$

[Si l'on autorisait 1 ou des nombres négatifs à être premier, on perdrait l'unicité (à l'ordre des facteurs près) de la factorisation du théorème fondamental de l'arithmétique, car par exemple $6 = 2 \cdot 3 = (-2)(-3) = 1 \cdot 2 \cdot 3$.]

Un **nombre composé** est un nombre z non nul qui est le produit de deux nombres strictement positifs qui ne sont ni ± 1 ni $\pm z$. Cette décomposition est possible dès que z a des diviseurs qui ne sont pas triviaux. Chaque entier plus grand que 1 est donc soit un nombre premier, soit un nombre composé. En pratique : Si $n > 0$ est composé, on peut l'écrire comme $n = t \cdot s$ avec t, s strictement entre 1 et n (où t, s sont bien évidemment des diviseurs de n).

Propriétés des nombres premiers :

• **"PGCD" :** Le PGCD de $a \in \mathbb{Z}$ et un nombre premier p est soit 1 (si $p \nmid a$) soit p (si $p \mid a$) [puisque l'on cherche un diviseur de p, on n'a pas beaucoup de choix].
Une conséquence : deux nombres premiers sont soit égaux soit premiers entre eux.

• **"Lemme d'Euclide" :** Si un nombre premier divise un produit, il divise au moins un des facteurs. [Preuve : Par itération en utilisant le fait que si $a \mid bc$ et $PGCD(a, b) = 1$ alors $a \mid c$.] Une conséquence : Si un nombre premier divise une puissance, il en divise la base.

• **"Le plus petit diviseur > 1" :** Si $n > 1$ n'est pas un nombre premier, le plus petit diviseur > 1 est $\leqslant \sqrt{n}$, et est un nombre premier. [Si n est un nombre premier, son plus petit diviseur > 1, étant n, est aussi un nombre premier.]

2 Décomposition en produit de facteurs premiers

Théorème fondamental de l'arithmétique : Tout nombre entier plus grand que 1 peut être écrit comme un produit de nombres premiers d'une unique façon, à l'ordre près des facteurs. Par exemple :

$$12 = 2 \cdot 2 \cdot 3 = 2 \cdot 3 \cdot 2 = 3 \cdot 2 \cdot 2$$

Petite remarque : Le nombre 1 est consideré comme le produit vide ; les nombres premiers sont des produits avec seulement un facteur ; 0 n'est pas un produit de nombres premiers. Si on prend les nombres premiers (pas leur puissances !) dans l'ordre croissant, et on regroupe les mêmes nombres comme une puissance, on obtient la *factorisation canonique*. Par exemple :

$$12 = 2^2 \cdot 3.$$

Avec cette factorisation on voit bien les diviseurs premiers et leur multiplicité.

• La plus grande puissance d'un nombre premier p qui divise un nombre $n \geqslant 1$ est exactement la puissance de p que l'on trouve dans la factorisation canonique de n (si p est un nombre premier qui ne divise pas n, cette puissance est $p^0 = 1$).

Pour mieux comparer les nombres, il est préférable d'utiliser dans la notation tous les nombres premiers :

$$12 = 2^2 \cdot 3^1 \cdot 5^0 \cdot 7^0 \cdot 11^0 \dots$$

On peut donc écrire en entier $a \geqslant 1$ comme

$$a = \prod_{p \in \mathcal{P}} p^{a_p} ,$$

où les exposants a_p sont des entiers qui sont positifs ou nuls. Par exemple, si $a = 12$ on trouve $a_2 = 2$, $a_3 = 1$, et $a_p = 0$ lorsque $p \geqslant 5$. Pour le nombre 1, tout exposant est nul.

3 Critères avec les exposants

Soient a, b des entiers strictement positifs et écrivons leurs factorisations canoniques avec toutes nombres premiers :

$$a = \prod_{p \in \mathcal{P}} p^{a_p} \qquad b = \prod_{p \in \mathcal{P}} p^{b_p}$$

• **Diviseurs premiers :** Les nombres premiers p tels que $a_p > 0$ sont exactement les diviseurs premiers de a.

• **Égalité :** On a $a = b$ si et seulement si $a_p = b_p$ pour tout $p \in \mathcal{P}$.

• **Divisibilité :** On a $a \mid b$ si et seulement si $a_p \leqslant b_p$ pour tout $p \in \mathcal{P}$.

• **Produit et Quotient :** La factorisation canonique de ab et (si b divise a) de $\frac{a}{b}$ sont :

$$ab = \prod_{p \in \mathcal{P}} p^{a_p + b_p} \qquad \frac{a}{b} = \prod_{p \in \mathcal{P}} p^{a_p - b_p}\,.$$

• **Puissances :** Un nombre entier strictement positif est une puissance n-ième si et seulement si touts exposants de sa factorisation canonique sont divisible par n (pour les nombres négatifs, il faut faire attention, car ils ne peuvent jamais être des puissances n-ième avec n pair).

• **PGCD et PPCM :** La factorisation canonique du $PGCD$ et $PPCM$ sont

$$PGCD(a,b) = \prod_{p \in \mathcal{P}} p^{\min(a_p, b_p)} \qquad PPCM(a,b) = \prod_{p \in \mathcal{P}} p^{\max(a_p, b_p)}\,.$$

En particulier, on a des nombres premiers entre eux si et seulement si pour chaque p on a $a_p = 0$ ou $b_p = 0$ (il faut que le minimum des exposants soit 0).

• **Somme :** Si $a_p \neq b_p$, l'exposant de p pour la somme $a+b$ est $\min\{a_p, b_p\}$. Par exemple, la plus grands puissance de 2 qui divise $24 + 16$ est 2^3.
Par contre, si $a_p = b_p$ l'exposant cherché est au moins ce nombre, mais peut même être très grand. Par exemple, la plus grand puissance qui divise $1 + 31$ est 2^5.

• **Nombre des diviseurs :** Soit a un nombre entier strictement positif. Le nombre de diviseurs positifs de a est

$$\prod_{p \in \mathcal{P}} (a_p + 1)$$

[Idée de la preuve : On détermine un diviseur avec les exposants de sa factorisation en produit de nombres premiers, et l'exposant de p peut varier de 0 à a_p (il y a $a_p + 1$ possibilités). Ensuite, les choix des exposants sont indépendants.] Par exemple, le nombre $60 = 2^2 \cdot 3^1 \cdot 5^1$ a $3 \cdot 2 \cdot 2 = 12$ diviseurs positifs.

• Pour le produit, le PGCD, et le PPCM de plusieurs nombres on a des formules analogues. À noter : Le PGCD de tous les nombres est 1 si et seulement si pour chaque nombre premier p on trouve au moins un exposant pour p qui est 0. Si les nombres sont aussi premiers entre eux deux à deux, on a au plus un exposant pour p qui est non nul. On vois bien que "premiers entre eux deux à deux" est une condition plus forte que "le PGCD est 1".