Arithmétique – Partie 3 : Nombres premiers

Savoir.

- ☐ Connaître la définition de nombre premier.
- ☐ Savoir qu'il en existe une infinité.
- ☐ Connaître le lemme d'Euclide.

Savoir-faire.

- ☐ Savoir calculer une décomposition en facteurs premiers.
- ☐ Savoir en déduire des pgcd et ppcm.

Les nombres premiers

— **Définition.** Un **nombre premier** est un entier naturel supérieur ou égal à 2 qui n'est divisible que par 1 et par lui-même.

— *Exemple.* $2, 3, 5$ ou encore 17 sont des nombres premiers. En revanche $9 = 3 \times 3$ ou encore $14 = 2 \times 7$ ne sont pas premiers.

— **Lemme.** Tout entier naturel $n \geqslant 2$ admet un diviseur premier.

— *Démonstration.* Si n est lui-même premier, il n'y a rien à démontrer (car n se divise lui-même).
Sinon, cela signifie que n admet un diviseur strictement compris entre 1 et n. Notons $\mathscr{D}$ l'ensemble des diviseurs de n strictement compris entre 1 et n. Cet ensemble d'entiers est non vide, donc il possède un plus petit élément, que nous noterons p.
Supposons par l'absurde que p ne soit pas premier, alors il possède lui-même un diviseur q strictement compris entre 1 et p. Mais $q|p$ et $p|n$ donc $q|n$. Ainsi q est un diviseur de n (qui n'est pas 1) et qui est plus petit que p. Ceci est une contradiction car p est le plus petit diviseur de n.
Donc p est premier, et par conséquent n est bien divisible par un nombre premier.

Théorème (Euclide).

Il existe une infinité de nombres premiers.

Démonstration. Voilà la démonstration d'Euclide, par l'absurde :
Supposons que l'ensemble des nombres premiers soit fini : on les note alors $p_1, p_2, ..., p_n$. Soit

$$N := p_1 \times p_2 \times \cdots \times p_n \ + 1 = \prod_{i=1}^{n} p_i \ + \ 1$$

N admet un diviseur premier d'après le lemme précédent. Notons p_k un tel diviseur. $p_k|N$, mais $p_k|(\prod_{i=1}^{n} p_i)$ donc $p_k|N - (\prod_{i=1}^{n} p_i) = 1$. Ainsi $p_k|1$ donc $p_k = 1$ ce qui est une contradiction avec $p_k \geqslant 2$.
Ceci démontre par l'absurde que l'ensemble des nombres premiers est infini.

Lemme d'Euclide

Lemme d'Euclide. Soit p un nombre premier et a et b deux entiers.

Si $p|ab$, alors $p|a$ ou $p|b$.

Démonstration. Supposons que p ne divise pas a. Ceci signifie que $\text{pgcd}(p, a) = 1$ puisque les seuls diviseurs de p sont p et 1. On applique le lemme de Gauss : $p|ab$ et $\text{pgcd}(p, a) = 1 \implies p|b$.

Exercice. Soit p un nombre premier, montrer que $\sqrt{p}$ n'est pas un rationnel en utilisant le lemme de Gauss.

Décomposition en produit de facteurs premiers

Décomposition en produit de facteurs premiers. Soit un entier $n \geqslant 2$. Il existe une unique suite de nombres premiers $p_1 < p_2 < \cdots < p_k$ et une unique suite d'exposants entiers positifs non nuls $\alpha_1, \alpha_2, ..., \alpha_k$ tel que :

$$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \cdots \times p_k^{\alpha_k} = \prod_{i=1}^{k} p_i^{\alpha_i}$$

Remarques.

— Les démonstrations de l'existence et de l'unicité de cette décomposition peuvent s'effectuer par récurrence.

— L'entier n admet au moins un facteur premier p_i tel que $p_i \leqslant \sqrt{n}$; si ce n'est pas le cas, cela signifie que n est premier ! Ceci est pratique pour démontrer qu'un nombre fixé est premier ou non.

Exemples.

— Le nombre 271 est un nombre premier. En effet, il n'est pas divisible par $2, 3, 5, 7, 11$ ou 13. Et cela suffit à assurer qu'il est premier puisque $\sqrt{271} \simeq 16,5 < 17$

— Recherchons la décomposition en facteurs premiers de 1 188 :

$$1\,188 = 2 \times 594 = 2^2 \times 297 = 2^2 \times 3 \times 99 = 2^2 \times 3^2 \times 33 = 2^2 \times 3^3 \times 11$$

Et cette dernière égalité est bien la décomposition en facteurs premiers.

pgcd

Proposition. Soient deux entiers $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ et $m = \prod_{i=1}^{k} p_i^{\beta_i}$ (avec α_i et β_i éventuellement nuls). On a alors :

$$\begin{cases} \text{pgcd}(n,m) & = \prod_{i=1}^{k} p_i^{\min(\alpha_i,\beta_i)} \\ \text{ppcm}(n,m) & = \prod_{i=1}^{k} p_i^{\max(\alpha_i,\beta_i)} \end{cases}$$

En d'autres termes, on compare les exposants des nombres entiers p présents dans les décompositions de m et de n. Le plus petit exposant (c'est éventuellement 0) sera celui de $\text{pgcd}(n,m)$, et le plus grand exposant est celui de $\text{ppcm}(n,m)$.

Exemple. Reprenons l'exemple de 1 188 et de 120.

— On a déjà obtenu la décomposition en facteurs premiers de $1\,188 = 2^2 \times 3^3 \times 11$.

— Recherchons celle de 120 : $120 = 2 \times 60 = 2^2 \times 30 = 2^3 \times 15 = 2^3 \times 3 \times 5$.

— Réécrivons les décompositions en faisant apparaître tous les facteurs premiers présents dans au moins l'une des décompositions :

$$\begin{cases} 1\,188 & = 2^2 \times 3^3 \times 5^0 \times 11^1 \\ 120 & = 2^3 \times 3^1 \times 5^1 \times 11^0 \end{cases}$$

On obtient alors leur pgcd et leur ppcm en choisissant respectivement le plus petit et le plus grand des exposants pour chaque facteur premier :

$$\begin{cases} \text{pgcd}(1\,188, 120) & = 2^2 \times 3^1 \times 5^0 \times 11^0 = 4 \times 3 = 12 \\ \text{ppcm}(1\,188, 120) & = 2^3 \times 3^3 \times 5^1 \times 11^1 = 8 \times 27 \times 5 \times 11 = 11\,880 \end{cases}$$

Exercice. Déterminer les décompositions en produit de facteurs premiers de 585 et de 247, puis en déduire leur pgcd et leur ppcm.