LES NOMBRES PREMIERS

I. Définition et premières propriétés

1 Nombres premiers dans $\mathbb{N}$

DÉFINITION Dire qu'un nombre entier naturel est premier signifie qu'il admet exactement deux diviseurs dans $\mathbb{N}$: 1 et lui-même.

EXEMPLES :
- 0 n'est pas premier, car il admet une infinité de diviseurs dans $\mathbb{N}$.
- 1 n'est pas premier, car il a un seul diviseur dans $\mathbb{N}$: lui-même.
- 2 est le plus petit nombre premier et le seul qui soit pair.

2 Reconnaissance d'un nombre premier

LEMME n désigne un nombre entier naturel supérieur ou égal à 2.
Si n n'est pas premier, alors n admet au moins un diviseur premier p : son plus petit diviseur dans $\mathbb{N}$ autre que 1, tel que $2 \leqslant p \leqslant \sqrt{n}$.

DÉMONSTRATION

$n \geqslant 2$ est un nombre entier naturel non premier. L'ensemble de ses diviseurs strictement supérieurs à 1 contient au moins un élément différent de n. On note p le plus petit de ces diviseurs.
On raisonne par l'absurde et **on suppose que p n'est pas premier**. Alors p admet un diviseur d tel que $1 < d < p$. De d divise p et p divise n, on déduit que d divise n, ce qui établit une contradiction, car p est le plus petit diviseur de n strictement supérieur à 1. Ainsi, p **est premier**.
Il reste à démontrer que p vérifie $2 \leqslant p \leqslant \sqrt{n}$. On sait que $n = pq$ avec $1 < p \leqslant q$ donc $p^2 \leqslant pq$ soit $p^2 \leqslant n$ et par suite, $p \leqslant \sqrt{n}$.

PROPRIÉTÉ n désigne un nombre entier naturel, $n \geqslant 2$.
Si n n'est divisible par aucun nombre premier p tel que $2 \leqslant p \leqslant \sqrt{n}$, alors n est premier.

DÉMONSTRATION

C'est la contraposée du lemme précédent.

EXEMPLE : 157 est-il premier ?
Les nombres premiers inférieurs à $\sqrt{157}$ ($\sqrt{157} \approx 12{,}5$) sont 2, 3, 5, 7, 11.
157 n'est divisible par aucun de ces nombres.
Donc 157 est premier.

3 L'ensemble des nombres premiers

PROPRIÉTÉ Il existe une infinité de nombres premiers.

DÉMONSTRATION

On raisonne par l'absurde. On suppose qu'il existe un nombre fini de nombres premiers $p_1, p_2, \ldots, p_n$.
On considère le nombre $a = p_1\, p_2 \ldots p_n + 1$. Ce nombre entier naturel est supérieur ou égal à 2, il admet donc au moins un diviseur premier p_i parmi les nombres $p_1, p_2, \ldots, p_n$. Cet entier p_i divise a et divise $p_1\, p_2 \ldots p_n$, donc il divise la différence, c'est-à-dire 1. D'où la contradiction.
Ainsi, il existe une infinité de nombres premiers.

II. Décomposition en facteurs premiers

1 Existence et unicité d'une décomposition

PROPRIÉTÉ Tout nombre entier naturel $n \geqslant 2$ est premier ou produit de nombres premiers.

DÉMONSTRATION

Si n est premier, la propriété est établie.

Si n n'est pas premier, alors son plus petit diviseur $p_1 \geqslant 2$ est premier et il existe un nombre entier naturel n_1 tel que $n = p_1 n_1$ avec $n_1 < n$.

Si n_1 est premier, la propriété est établie.

Si n_1 n'est pas premier, alors on recommence comme précédemment.

De proche en proche, on obtient ainsi une suite strictement décroissante de nombres entiers naturels n_i tels que $1 \leqslant \ldots < n_i < \ldots < n_2 < n_1$. Cette suite est finie et le dernier d'entre eux est nécessairement égal à 1, donc $n = p_1 p_2 \ldots p_k$ avec $p_1, p_2, \ldots, p_k$ premiers.

Notation : Les nombres premiers ci-dessus ne sont pas nécessairement distincts. En les regroupant, on obtient $\boldsymbol{n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}}$ où $p_1, p_2, \ldots, p_r$ sont des nombres premiers et $\alpha_1, \alpha_2, \ldots, \alpha_r$ des nombres entiers naturels non nuls. On dit alors que ***n* est décomposé en produit de facteurs premiers**.

PROPRIÉTÉ La décomposition en produit de facteurs premiers de tout nombre entier naturel supérieur ou égal à 2 est unique.

DÉMONSTRATION

On suppose qu'un certain nombre premier p apparaît avec l'exposant $\alpha \geqslant 1$ dans une décomposition de n, et l'exposant $\beta \geqslant 0$ dans une autre (on envisage $\beta = 0$ pour le cas où p ne figurerait pas dans la deuxième composition). On a alors $n = p^\alpha a = p^\beta b$, où a et b sont des produits de nombres premiers distincts de p. Si $\alpha > \beta$, $p^{\alpha-\beta} a = b$, ce qui contredit que p et b sont premiers entre eux.

Si $\alpha < \beta$, $a = p^{\beta-\alpha} b$, ce qui contredit que p et a sont premiers entre eux. Donc $\alpha = \beta$.

2 Diviseurs d'un nombre entier naturel non premier

PROPRIÉTÉ $p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$ est la décomposition en facteurs premiers d'un nombre entier naturel n.
Les diviseurs de n sont de la forme $p_1^{\alpha'_1} p_2^{\alpha'_2} \ldots p_r^{\alpha'_r}$ où $0 \leqslant \alpha'_1 \leqslant \alpha_1, \ldots, 0 \leqslant \alpha'_r \leqslant \alpha_r$.

DÉMONSTRATION

- Les nombres entiers de la forme $p_1^{\alpha'_1} p_2^{\alpha'_2} \ldots p_r^{\alpha'_r}$ sont des diviseurs de n. En effet, on peut écrire : $n = (p_1^{\alpha'_1} p_2^{\alpha'_2} \ldots p_r^{\alpha'_r}) \times p_1^{\alpha_1 - \alpha'_1} p_2^{\alpha_2 - \alpha'_2} \ldots p_r^{\alpha_r - \alpha'_r}$ où les exposants $\alpha_i - \alpha'_i$ sont positifs ou nuls.
- d est un diviseur de n. Si $p^{\alpha'}$ avec p premier, divise d, alors $p^{\alpha'}$ divise n. L'unicité de la décomposition de n en facteurs premiers implique que le nombre $p^{\alpha'}$ doit figurer dans cette décomposition, donc p est l'un des p_i et $0 \leqslant \alpha' \leqslant \alpha_i$.

Ainsi d est de la forme $p_1^{\alpha'_1} p_2^{\alpha'_2} \ldots p_r^{\alpha'_r}$ où $0 \leqslant \alpha'_1 \leqslant \alpha_1, \ldots, 0 \leqslant \alpha'_r \leqslant \alpha_r$.

Conséquence

a et b désignent deux nombres entiers naturels supérieurs ou égaux à 2.

Le PGCD de *a* et *b* est égal au produit des facteurs premiers communs aux décompositions de *a* et *b*, chacun d'eux étant affecté du plus petit exposant avec lequel il figure dans *a* et *b*.

Source : Hyperbole Term S spécialité, éd. Nathan (programme 2012)