

Nombres premiers

Plein de choses intéressantes là : <https://www.futura-sciences.com/sciences/dossiers/mathematiques-merveilleux-nombres-premiers-1791/page/6/>

Définition : un nombre naturel est premier s'il possède exactement deux diviseurs : 1 et lui-même.

1 n'est pas premier.

Définition : un diviseur propre de n est un diviseur de n différent de 1 et de n .

Remarque : on peut dire qu'un entier négatif est premier si son opposé est premier. Dans la suite de ce chapitre, on ne s'intéressera qu'aux nombres entiers strictement positifs.

Propriété : si un nombre n n'a pas de diviseur propre inférieur ou égal à $\sqrt{n}$, alors ce nombre est premier.

On peut vérifier la contraposée sur quelques exemples.

25 n'est pas premier et on peut vérifier que 25 possède le diviseur propre 5 qui est inférieur ou égal à $\sqrt{25}$.

21 n'est pas premier et on peut vérifier que 21 possède le diviseur propre 3 qui est inférieur ou égal à $\sqrt{21}$. On peut remarquer que si 21 est le produit de deux nombres différents, alors un de ces nombres est inférieur à $\sqrt{21}$, l'autre est supérieur à $\sqrt{21}$.

Démonstration : soit n un nombre qui n'a pas de diviseur propre inférieur ou égal à $\sqrt{n}$.

Raisonnons par l'absurde : supposons que n n'est pas premier. Il existe alors deux nombres p et q (distincts ou égaux) différents de 1 et de n tels que $n = pq$.

n n'a pas de diviseur propre inférieur ou égal à $\sqrt{n}$, donc $p > \sqrt{n}$ et $q > \sqrt{n}$, donc $pq > n$, absurde car $n = pq$.

Décomposition d'un entier en produit de nombre premiers

Exemples : $24 = 2 \times 2 \times 2 \times 3 = 2^3 \times 3$. C'est la décomposition en produit de facteurs premiers de 24.

On peut aussi écrire que $24 = 3 \times 2^3$ mais, si l'on range les facteurs premiers du plus petit au plus grand, il n'y a pas d'autre décomposition de 24 (on le démontrera).

Comparons deux décompositions : $24 = 2^3 \times 3$ et $20 = 2^2 \times 5$.

On voit que les diviseurs communs de 20 et de 24 sont 2 et 2^2 . On voit encore plus facilement que $\text{PGCD}(20; 24) = 4$.

De même, le PGCD de $2250 = 2 \times 3^2 \times 5^3$ et de $2835 = 3^4 \times 5 \times 7$ est $3^2 \times 5 = 45$.

De même, en comparant $24 = 2^3 \times 3$ et $175 = 5^2 \times 7$, on voit facilement que 24 et 175 n'ont pas de diviseur propre en commun donc que $\text{PGCD}(24; 175) = 1$ et que 24 et 175 sont premiers entre eux.

Enfin, la décomposition d'un nombre premier en produit de facteur premier est simple : $37 = 37$.

Propriété : un nombre $n \geq 2$ est soit premier, soit le produit de nombres premiers.

Démonstration : Raisonnons par l'absurde : supposons qu'il existe des nombres supérieurs à 2 qui ne soient pas premiers et qui ne soient pas le produit de nombres premiers.

Soit m le plus petit d'entre eux. Cela signifie que tout nombre strictement inférieur à m est soit premier, soit le produit de nombres premiers.

m n'est pas premier donc il existe deux nombres p et q tels que $m = pq$ et tels que $2 \leq p < m$ et $2 \leq q < m$.

$p < m$ donc p est soit premier soit le produit de nombre premiers. Même chose pour q .

$m = pq$ est donc le produit de nombres premiers. Absurde car on a supposé que m n'est pas premier et n'est pas le produit de nombres premiers.

Conséquence : tout entier $n \geq 2$ admet au moins un diviseur premier.

Conséquence : tout entier $n \geq 2$ s'écrit $n = p_1^{a_1} \times p_2^{a_2} \times \dots \times p_m^{a_m}$ où les p_i sont des nombres premiers et les a_i des entiers positifs non nuls.

a_i s'appelle la multiplicité de p_i dans cette décomposition.

Exemple : $237.576.240 = 2^4 \times 3^5 \times 5 \times 11^2 \times 101$.

La multiplicité de 3 dans cette décomposition est 5.

Propriété : si $p_1 < p_2 < \dots < p_m$, alors cette décomposition est unique.

Cette écriture est la décomposition de n en produit de facteurs premiers.

Démonstration : raisonnons par récurrence sur n .

Initialisation : la propriété est vraie pour $n = 2$.

Hérédité : supposons que la propriété est vraie pour tout entier compris entre 2 et $n - 1$ et montrons qu'elle est vraie pour n .

Supposons qu'il existe deux décompositions : $n = p_1 \times p_2 \times \dots \times p_m$ et $n = q_1 \times q_2 \times \dots \times q_r$ (les entiers p_i peuvent être égaux mais sont rangés du plus petit au plus grand, pareil pour les q_i).

Montrons que $p_1 = q_1$. Pour cela, montrons qu'il est impossible que $p_1 < q_1$ et que $p_1 > q_1$.

Supposons que $p_1 < q_1$.

q_1 est le plus petit des q_i donc p_1 n'est égal à aucun des q_i .

p_1 divise n donc p_1 divise le produit $q_1 \times q_2 \times \dots \times q_r$.

p_1 et q_1 sont tous les deux premiers donc ils sont premiers entre eux donc, d'après le théorème de Gauss, p_1 divise le produit $q_2 \times \dots \times q_r$.

$q_2 \times \dots \times q_r < n$ donc, par l'hypothèse de récurrence, cette décomposition est unique donc, puisque p_1 est premier, p_1 est égal à l'un des q_i ($i > 1$), ce qui est absurde car on a montré que p_1 n'est égal à aucun des q_i .

Supposons que $p_1 > q_1$.

On montre de la même façon que q_1 n'est égal à aucun des p_i et que q_1 est égal à l'un des p_i , ce qui est absurde.

On a donc montré que $p_1 = q_1$.

On divise par p_1 et on trouve $p_2 \times \dots \times p_m = q_2 \times \dots \times q_r$.

Ces deux entiers sont égaux et inférieurs à n donc, par hypothèse de récurrence, on a l'unicité.

Propriété : il existe une infinité de nombres premiers.

Lemme : soit n un entier, soit un entier $p \geq 2$. Si p divise n , alors p ne divise pas $n + 1$.

Démonstration du lemme : si $p \mid n$ et $p \mid (n + 1)$, alors $p \mid (n + 1 - n)$, alors $p \mid 1$, alors $p = 1$. Absurde car $p \geq 2$.

Démonstration du théorème : supposons qu'il existe un nombre fini de nombres premiers.

Soit p un nombre premier et n le produit de tous ces nombres premiers.

$n + 1$ est supérieur à n'importe quel nombre premier donc $n + 1$ n'est pas premier.

p divise n donc p ne divise pas $n + 1$. On démontre de même qu'aucun nombre premier ne divise $n + 1$ donc $n + 1$ n'a pas de diviseur premier donc $n + 1$ est premier. Absurde.

Remarque : grâce à un arbre, à partir de la liste des diviseurs premiers, on peut donner la liste des diviseurs.