Chapitre 2 : Nombres Premiers

C. Aupérin

2009-2010

"Télécharger c'est tuer l'industrie, tuons les tous" Thurston Moore

Dernière modification : 9 novembre 2009

Table des matières

COURS : NOMBRES PREMIERS

1 Définition

Travail de l'élève : Activités 1 + 2 + 3 p 36

Définition 1. On dit qu'un entier naturel p est premier s'il possède exactement 2 diviseurs positifs : 1 et lui-même.

Remarques :

- Tout entier naturel différent de 1 admet *au moins* deux diviseurs : 1 et lui-même
- Ne pas confondre nombre premier et nombres premiers entre eux.
- Si p est un nombre premier et n un entier naturel, alors soit p divise n, soit p est premier avec n.

Exemples :

- 0 n'est pas premier car il admet une infinité de diviseurs
- 1 n'est pas premier car il n'admet qu'*un seul* diviseur : lui-même.
- 2 est le seul nombre premier pair (les autres sont divisibles au moins par 1, eux-mêmes et 2).
- 3, 5, 7, 11, 13 sont des nombres premiers (voir la table p 156)
- 6 n'est pas un nombre premier, car il est divisible par 1, 6, 2 et 3.

THÉORÈME 1. Soit $n \in \mathbb{N}$ supérieur ou égal à 2. Alors :
- n admet au moins un diviseur premier
- Si n n'est pas premier, alors il admet au moins un diviseur premier p tel que $p \leq \sqrt{n}$.

Preuve : Si n est premier, alors il s'admet lui-même comme diviseur premier.
Sinon, n admet au moins un diviseur propre. Supposons tous les diviseurs de n soient supérieurs strictement à $\sqrt{n}$. Alors il existe $a > \sqrt{n}$ et $b > \sqrt{n}$ tels que $a \times b = n$ mais $a \times b > \sqrt{n}^2 = n$. Ce qui est absurde.

Corollaire 1. Soit $n \in \mathbb{N}$ supérieur ou égal à 2. Alors si n n'admet aucun diviseur inférieur ou égal à sa racine carré, alors n est premier

Démonstration :

C'est la contraposée du théorème.

Lire le Point Info de la page 40 et la spirale p 41
TP 1 46 : Crible d'Eratosthène

Exercices du livre n° 3 + 4 p 51

THÉORÈME 2. Il existe une infinité de nombres premiers.

Démonstration :

Supposons qu'il existe un nombre fini n de nombres premiers, notés p_1, p_2, $\dots$, p_n. On pose $N = p_1 \times p_2 \times \cdots \times p_n + 1$.
Alors si N est premier, on a trouvé un autre nombre premier, l'hypothèse de départ est donc absurde.
Si N n'est pas premier, alors il admet un certain diviseur premier k. Si $k = p_i$ alors $k|p_1p_2\dots p_n$ et $k|N$ donc $k|1$ (la différence). Donc $k = 1$, mais k est premier donc c'est impossible.
Par conséquent on a trouvé un autre nombre premier, l'hypothése est absurde.
Dans les deux cas possibles, l'hypothèse est absurde, donc elle l'est toujours.

2 Décomposition en nombres premiers

THÉORÈME 3. Tout entier naturel supérieur ou égal à deux est :
- Soit un nombre premier
- Soit un produit de puissance de nombres premiers.

Cette écriture, appelée *décomposition en nombres premiers* est unique à l'ordre des facteurs près.

Démonstration :

Supposons n non premier.
Existence :
Soit $n \geq 2$. D'après le théorème précédent, n admet un diviseur premier p_1 et l'on a $n = p_1n_1$ avec $2 \leq n_1 < n$ (n n'est pas premier donc $n_1 \neq 1$).
Par le théorème précédent, on a de même que n_1 admet un diviseur premier p_2 et que $n = p_1p_2n_2$ avec $1 \leq n_2 < n_1 < n$. Si $n_2 = 1$ alors n_1 est premier et le résultat est démontré. Sinon on réitère le raisonnement tant que le quotient est différent de 1. La liste des quotients est une liste décroissante d'entiers naturels, elle admet donc un plus petit élément n_k et est finie. On a alors $n = p_1p_2\dots p_k$
Unicité : Admise pour l'instant (cf exo 24 p 81)

Exemples : On utilise les critères de divisibilité. $105 = 3 \times 5 \times 7$; $83160 = 2^3 \times 3^3 \times 5 \times 7 \times 11$.

Exercices du livre n° 5 + 7 + 8 p 51

THÉORÈME 4. Soit n un entier naturel supérieur ou égal à 2 se décomposant en produit de facteurs premiers sous la forme $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$.
Les diviseurs positifs de n sont les nombres de la forme $p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$, avec $0 \leq \beta_i \leq \alpha_i$ pour tout $1 \leq i \leq k$.

Démonstration :

Il est clair que les nombres de cette forme divisent n car $\alpha_i - \beta_i \geq 0$ pour tout $1 \leq i \leq k$.
Démontrons maintenant que tout diviseur de n est de cette forme.
Soit d un diviseur de n. Alors il existe un entier d' tel que $n = d \times d'$. Le produit des décompositions en facteurs premiers de d et d' est une décomposition en produit de facteurs premiers de n.
Comme elle est unique, c'est la même.
Les seuls diviseurs premiers intervenant dans les décompositions de d et d' sont donc les p_i et leur exposant ne peuvent être qu'inférieurs ou égaux aux α_i.
L'entier d est donc forcément de la forme indiquée.

Corollaire 2. Soit un entier $n \leq 2$ se décomposant en produit de facteurs premiers sous la forme $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$.
Alors, n possède $(\alpha_1 + 1) \times (\alpha_2 + 1) \times \cdots \times (\alpha_k + 1)$ diviseurs positifs.

Démonstration :

Dénombrement.

Exercices du livre n° 9 + 10 + 11)1.+ 13 + 14 + 15 p 51

Exercices du livre n° 18 à 22 + 24 ? + 31 + 32 + 33 + 34 + 37 + 40 p 52

Exercices du livre n° 43 + 45 + 48 p 54