

Les nombres premiers

I Caractérisation

Définition : Un entier naturel p est premier s'il possède exactement deux diviseurs positifs : 1 et p .

Corollaire : Un entier naturel p est premier si, et seulement si, $D^+(p) = \{1; p\}$.

Exemples :

- 1 n'est pas premier puisqu'il ne possède qu'un seul diviseur positif.
- 2 et 3 sont premiers puisque $D^+(2) = \{1; 2\}$ et $D^+(3) = \{1; 3\}$.
- 6 n'est pas premier puisque $D^+(6) = \{1; 2; 3; 6\}$

Propriétés : Soit n un entier naturel, $n \geq 2$,

- n admet au moins un diviseur premier p ;
- Si n n'est pas premier alors n admet au moins un diviseur premier $p \leq \sqrt{n}$.

Démonstration 1

Conséquence : **Test de primalité d'un nombre entier**

Soit n un entier naturel, $n \geq 2$,

si n n'est divisible par aucun des nombres premiers inférieurs ou égaux à \sqrt{n} alors n est un nombre premier.

Exercice 1 : Écrire un algorithme qui teste puis affiche si un nombre entier naturel est premier.

Programmer cet algorithme et le faire fonctionner.

Propriété : Il existe une infinité de nombres premiers.

Démonstration 2 *Démonstration d'Euclide*

II Décomposition en facteurs premiers

Théorème : **Théorème fondamental de l'arithmétique**

Tout entier naturel supérieur ou égal à 2 se décompose en produit de facteurs premiers.

De plus, cette décomposition est unique à l'ordre près des facteurs.

Soit $n \in \mathbb{N}$, $n \geq 2$ alors $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \dots \times p_k^{\alpha_k}$ avec p_1, p_2, \dots, p_k des nombres premiers et $\alpha_1, \alpha_2, \dots, \alpha_k$ des entiers naturels non nuls.

Démonstration 3

Exercice 2 : Méthode pour obtenir la décomposition en facteurs premiers de 140.

Propriétés : Soit $n \in \mathbb{N}$, $n \geq 2$ alors, en reprenant les notations du théorème précédent :

- Les diviseurs positifs de n sont les entiers $p_1^{\beta_1} \times p_2^{\beta_2} \times \dots \times p_k^{\beta_k}$ où $0 \leq \beta_1 \leq \alpha_1$, $0 \leq \beta_2 \leq \alpha_2, \dots, 0 \leq \beta_k \leq \alpha_k$;
- Le nombre de diviseurs positifs de n est donc $(\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_k + 1)$.

Exercice 3 :

- 1) Calculer le nombre de diviseurs de 140.
- 2) Écrire la forme générale d'un diviseur de 140.
- 3) Représenter l'arbre des diviseurs de 140.

Exercice 4 : Écrire un algorithme qui donne la décomposition en facteur premiers d'un entier naturel.

Programmer cet algorithme et le faire fonctionner.

III PPCM et PGCD de deux entiers

Définition : Soit m et n deux entiers non nuls, on appelle PPCM de m et n le **plus petit multiple commun** strictement positif de m et de n . On note cet entier PPCM(m, n).

Exercice 5 : Déterminer PPCM(25, 15) puis PPCM(7, 13).

Exercice 6 : Démontrer que le PPCM de deux nombres premiers distincts est leur produit.

Propriété : Soit m et n deux entiers naturels, $m \geq 2$ et $n \geq 2$ et leur décomposition sur **les mêmes** nombres premiers, p_1, p_2, \dots, p_k , en autorisant les exposants nuls.

$$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \dots \times p_k^{\alpha_k} \text{ avec } \alpha_1, \alpha_2, \dots, \alpha_k \text{ des entiers naturels,}$$

$$m = p_1^{\beta_1} \times p_2^{\beta_2} \times \dots \times p_k^{\beta_k} \text{ avec } \beta_1, \beta_2, \dots, \beta_k \text{ des entiers naturels.}$$

Alors :

<ul style="list-style-type: none"> • $\text{PGCD}(m, n) = p_1^{\min(\alpha_1, \beta_1)} \times p_2^{\min(\alpha_2, \beta_2)} \times \dots \times p_k^{\min(\alpha_k, \beta_k)}$, • $\text{PPCM}(m, n) = p_1^{\max(\alpha_1, \beta_1)} \times p_2^{\max(\alpha_2, \beta_2)} \times \dots \times p_k^{\max(\alpha_k, \beta_k)}$.
--

Exercice 7 :

- 1) Déterminer la décomposition en facteurs premiers de 294.
- 2) En déduire le PPCM et le PGCD de 140 et 294.

IV Petit théorème de Fermat¹

Théorème : Soit p un nombre premier et a un entier naturel non multiple de p , alors $a^{p-1} \equiv 1 [p]$.

Exemple : 13 est premier et ne divise pas 4 donc $4^{12} \equiv 1 [13]$.

Démonstration 4

Corollaire : Soit p un nombre premier alors, pour tout entier naturel a , $a^p \equiv a [p]$

Exemples : 7 est premier donc $\begin{cases} 10^7 \equiv 10 [7] \\ 14^7 \equiv 17 [7] \end{cases}$ d'où $\begin{cases} 10^7 \equiv 3 [7] \\ 14^7 \equiv 0 [7] \end{cases}$.

Démonstration 5

1. **Pierre de Fermat**, né dans la première décennie du XVII^e siècle, à Beaumont-de-Lomagne, près de Montauban, et mort le 12 janvier 1665 à Castres, est un magistrat, polymathe et surtout mathématicien français, surnommé « le prince des amateurs ». Il est aussi poète, habile latiniste et helléniste, et s'est intéressé aux sciences et en particulier à la physique; on lui doit notamment le principe de Fermat en optique. Il est particulièrement connu pour avoir énoncé le dernier théorème de Fermat, dont la démonstration n'a été établie que plus de 300 ans plus tard par le mathématicien britannique Andrew Wiles en 1994.