Chapitre 3 : Nombres premiers

Dans une lettre à Euler, Goldbach (1690-1764) conjecture que: « Tout nombre pair plus grand que 2 est somme de deux nombres premiers » personne- jusqu'à présent- n'a pu établir cette propriété… de là à se sentir pousser des ailes…

1. Nombres premiers :

1.1. Définition :

Un entier naturel p est premier s'il possède exactement deux diviseurs entiers naturels distincts : 1 et lui-même.

Propriétés immédiates :

- Tout entier relatif divise 0 donc 0 n'est pas premier.
- L'ensemble des diviseurs de 1 est $\{1\}$, donc 1 n'est pas premier.
- Un entier qui n'est pas premier est dit **composé.**

Test de primalité :

- Tout entier naturel n $(n \geq 2)$ admet un diviseur premier.
- Tout entier naturel n, distinct de 0 et 1 et non premier, admet au moins un diviseur premier p tel que $p^2 \leq n$.

Démonstration :

Soit n un entier non premier autre que 0 et 1.

L'ensemble D des diviseurs de n tels que $2 \leq d < n$ n'est pas vide. Il admet donc un plus petit élément p.

- *Montrons que ce nombre p est premier. En effet, s'il n'est pas premier, il possède un diviseur strict d tel que $2 \leq d < p$. Alors $d \mid p$ et $p \mid n$, donc $d \mid n$, avec $d < p$. d serait donc un diviseur de n strictement inférieur à p qui est le plus petit élément de D, ce qui est absurde. Donc p est premier.*
- *On a donc $n = p \times q$ avec $q \in D$ et donc $p \leq q$. D'où $p^2 \leq p \times q$ ie $p^2 \leq n$.*

En pratique, on applique cette propriété pour déterminer si un entier est premier : il suffit de tester sa divisibilité par les entiers premiers inférieurs à sa racine carrée.

Ex : 853 est-il premier ? et 703 ?

On effectue la division par les entiers premiers successifs, jusqu'à ce que le quotient soit inférieur ou égal au diviseur, ou que le reste soit nul.

	Diviseur	Quotient	Reste
703	2	x	≠0
	3	x	≠0
	5	x	≠0
	7	100	≠0
	11	63	≠0
	13	54	≠0
	17	41	≠0
	19	37	0

	Diviseur	Quotient	Reste
853	2	x	≠0
	3	x	≠0
	5	x	≠0
	7	121	≠0
	11	777	≠0
	13	65	≠0
	17	50	≠0
	19	44	≠0
	23	37	≠0
	29	29	≠0

Donc 703 n'est pas premier mais 853 l'est.

Le **crible d'Eratosthène** est l'une des plus anciennes méthodes utilisées pour déterminer la liste des entiers premiers entre 1 et 100 (par exemple). Cette méthode est cependant dévoreuse d'espace mémoire, mais reste raisonnable pour les nombres de taille raisonnable.

Exercice : Ecrire un algorithme permettant de tester si un entier donné est premier ou non.

1.2. Ensemble des nombres premiers :

Théorème : R💙C :

L'ensemble des nombres premiers est infini.

Démonstration : Par l'absurde. Soit $\mathbb{P}$ l'ensemble des nombres premiers. On suppose qu'il est fini et on note $p_1, p_2, p_3, \dots, p_n$ ses éléments.

On nomme N le nombre défini par $N = p_1p_2p_3 \dots p_n + 1$. N est un entier, et il est supérieur à tous les éléments de $\mathbb{P}$. Ainsi, N n'est pas premier. Il admet donc un diviseur premier p_k, élément de $\mathbb{P}$.

Ainsi p_k divise Net p_k divise $p_1p_2p_3 \dots p_n$. Par combinaison linéaire, $p_k$divise donc $N - p_1p_2p_3 \dots p_n = 1$. Ceci est absurde car le seul diviseur de 1 est 1 qui n'est pas premier. Donc l'hypothèse « $\mathbb{P}$ est fini » conduit à une absurdité. D'où $\mathbb{P}$ est fini.

1.3. Le théorème fondamental de l'Arithmétique :

Théorème :

Tout entier naturel n ($n \geq 2$) se décompose en un produit de facteurs premiers et cette décomposition est unique, à l'ordre des facteurs près.

Démonstration :

- *Unicité : admise conformément au programme*
- *Existence :*

- *Si n est premier, la propriété est évidente.*
- *Si n n'est pas premier, alors son plus petit diviseur $p_1 \geq 2$est premier, et il existe un entier naturel n_1 tel que $n = p_1n_1$, avec $n_1 < n$.*
- *Si n_1 est premier, la propriété est établie.*
- *Sinon, on recommence comme pour n : $n_1 = p_2n_2$ avec p_2 premier et $n_2 < n_1$.*
- *De proche en proche, on construit une suite d'entiers naturels n_i strictement décroissante. Cette suite est finie et le dernier élément est 1. On a donc $n = p_1p_2 \dots p_k$ où les p_i sont tous premiers, mais pas nécessairement distincts… En regroupant les facteurs égaux, il vient : $n = p_1^{\alpha_1}p_2^{\alpha_2} \dots p_j^{\alpha_j}$où les α_i sont des entiers naturels non nuls. Il s'agit de la décomposition en facteurs premiers de n.*

Exercice (une autre preuve) : Soit A l'ensemble des nombres entiers ($n \geq 2$) n'admettant pas de décomposition en facteurs premiers. Supposons que A est non vide et nommons n_0 son plus petit élément. Montrer que n_0 n'est pas premier et obtenir une contradiction. Conclusion ?

❖ Un peu d'histoire : 1903 : Réunion de la société américaine de Mathématiques sur « La factorisation des grands nombres ». FN Cole, sans un mot, écrit au tableau :

$$2^{67} - 1 = 147\,573\,952\,589\,676\,412\,927$$

Puis, dans un autre coin du tableau, il calcule le produit :

$$193\,707\,721 \times 761\,838\,257\,287$$

Les deux résultats coïncident. Toujours sans un mot Cole retourne s'asseoir sous les applaudissements. Une conjecture vieille de 250 ans « le nombre de Mersenne $2^{67} - 1$ est premier » vient de s'écrouler.

Applications

Soient a et b deux entiers non nuls. Si $a = p_1^{\alpha_1}p_2^{\alpha_2} \dots . p_s^{\alpha_s}$ et $b = p_1^{\beta_1}p_2^{\beta_2} \dots p_s^{\beta_s}$ où $p_1, p_2, \dots, p_n$ sont des nombres premiers distincts et les α_i, β_i des entiers positifs ou nuls, alors $\boldsymbol{a}$ **divise** $\boldsymbol{b}$ **si et seulement si pour tout** $\boldsymbol{i}$, $\boldsymbol{\alpha_i \leq \beta_i}$

En conséquence si $n = p_1^{\alpha_1}p_2^{\alpha_2} \dots . p_s^{\alpha_s}$, alors il admet $(\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_s + 1)$ diviseurs.

PGCD de a et b :

Soient a et b deux entiers non nuls. Si $a = p_1^{\alpha_1}p_2^{\alpha_2} \dots . p_s^{\alpha_s}$ et $b = p_1^{\beta_1}p_2^{\beta_2} \dots p_s^{\beta_s}$ où $p_1, p_2, \dots, p_n$ sont des nombres premiers distincts et les α_i, β_i des entiers positifs ou nuls, alors $\boldsymbol{PGCD(a,b) = p_1^{\gamma_1}p_2^{\gamma_2} \dots . p_s^{\gamma_s}}$ **avec** $\boldsymbol{\gamma_i = \min(\alpha_i, \beta_i)}$.