Chapitre 2

Le théorème fondamental de l'arithmétique et sa preuve

2.1 Les nombres premiers

Lorsqu'on cherche à factoriser des nombres naturels le plus possible, certains nombres se distinguent. Afin de mettre en évidence ce phénomène, factorisons quelques nombres.

$$12 = 2 \cdot 6 = 2 \cdot 2 \cdot 3 \qquad 30 = 2 \cdot 15 = 2 \cdot 3 \cdot 5$$
$$39 = 3 \cdot 13 \qquad 175 = 5 \cdot 35 = 5 \cdot 5 \cdot 7$$
$$187 = 11 \cdot 17 \qquad 67 = 1 \cdot 67$$

On voit émerger certains nombres qui ne se factorisent pas : ce sont les *nombres premiers*.

Définition

Un *nombre premier* est un nombre p dont la seule factorisation possible est $p = 1 \cdot p$.

Remarques

1. Convention : on déclare que le nombre 1 n'est pas un nombre premier.
2. Voici les 18 premiers éléments de l'ensemble des nombres premiers.

$$\mathcal{P} = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, \ldots\}$$

2.2 Le théorème fondamental de l'arithmétique

Théorème fondamental de l'arithmétique

Tout nombre naturel n plus grand que 1 se factorise de façon essentiellement unique en produit de nombres premiers.

2.2.1 Existence de la décomposition

Proposition

Soit $n \in \mathbb{N}$, $n > 1$.
Le plus petit diviseur de n différent de 1 est un nombre premier.

Preuve

Par l'absurde, supposons que le plus petit diviseur de n différent de 1, noté d, n'est pas premier. Ainsi, n ne pourrait pas être premier non plus (car si n est premier, alors son plus petit diviseur différent de 1 est lui-même) et le fait que d divise n se traduirait par

$$n = d \cdot m \qquad \text{avec } 1 < d \leqslant m < n$$

En effet, d étant le plus petit diviseur de n différent de 1, on a bien $d \leqslant m$. De plus, puisque d n'est pas premier, on a

$$d = a \cdot b \qquad \text{avec } 1 < a, b < d$$

Ainsi, on aurait

$$n = a \cdot b \cdot m \qquad \text{avec } 1 < a, b < d \leqslant m$$

Ce qui montre que a et b seraient des diviseurs de n différents de 1 plus petits que d. C'est une contradiction avec le fait que d est le plus petit diviseur de n différent de 1. □

Preuve de l'existence d'une décomposition en nombres premiers

Soit $n \in \mathbb{N}$, $n > 1$.

Si n est premier, alors n est sa propre décomposition en nombres premiers et la preuve est finie.

Par contre, si n n'est pas premier, alors son plus petit diviseur différent de 1, noté p_1 est premier. Ainsi

$$n = p_1 \cdot n_1 \qquad \text{avec } 1 < p_1 \leqslant n_1 < n$$

Si n_1 est premier, alors la décomposition en nombres premiers de n est

$$n = p_1 \cdot n_1$$

et la preuve est finie.

Par contre, si n_1 n'est pas premier, alors son plus petit diviseur différent de 1, noté p_2 est premier. Ainsi

$$n_1 = p_2 \cdot n_2 \qquad \text{avec } 1 < p_2 \leqslant n_2 < n_1$$

Si n_2 est premier, alors la décomposition en nombres premiers de n est

$$n = p_1 \cdot p_2 \cdot n_2$$

et la preuve est finie.

Par contre, si n_2 n'est pas premier, alors son plus petit diviseur différent de 1, noté p_3 est premier. Ainsi

$$n_2 = p_3 \cdot n_3 \qquad \text{avec } 1 < p_3 \leqslant n_3 < n_2$$

...

On se rend compte que l'on ne peut pas continuer ainsi indéfiniment puisqu'on aurait construit une suite décroissante de nombres n_i naturels tous plus grands que 1. Cette suite ne pourrait pas être infinie, donc il existe forcément un moment où le n_k sera premier et dans ce cas, la preuve sera finie. □

2.2.2 Unicité de la décomposition

Le lemme d'Euclide

Soit a et $b \in \mathbb{Z}$. Si p est un nombre premier qui divise ab, alors p divise a ou b.

Preuve

Cette preuve nécessite l'utilisation du théorème de Bezout (voir page 25). On distingue :

1. p divise a. Dans ce cas, c'est démontré !
2. p ne divise pas a. Dans ce cas, il faut démontrer que p divise b. Comme p est premier et que p ne divise pas a, alors $\text{pgcd}(p, a) = 1$. Par le théorème de Bezout, il existe deux nombres entiers x et y tels que $x \cdot p + y \cdot a = 1$.

   En multipliant cette équation par b, on obtient :

$$\underbrace{x \cdot p \cdot b}_{\text{divisible par } p} + \underbrace{y \cdot a \cdot b}_{\text{divisible par } p, \text{ car } p \text{ divise } ab} = b$$

   Donc b est divisible par p. □

Remarque

Soit p et q deux nombres premiers. Si p divise q, alors $p = q$.

Preuve

Si p divise q, alors il existe $m \in \mathbb{N}$ tel que $q = p \cdot m$. Comme q est premier et que $p \neq 1$ (car 1 n'est pas premier), on a $m = 1$ et $p = q$. □

Preuve de l'unicité de la décomposition en nombres premiers

Soit $n \in \mathbb{N}$, $n > 1$.
On suppose que n admet deux décompositions

$$n = p_1 \cdots p_m = q_1 \cdots q_{m'} \qquad \text{avec } m \leqslant m' \quad (m, m' \in \mathbb{N} \setminus \{0\})$$

On va montrer qu'à une permutation près, on retrouve les mêmes nombres premiers et qu'il y en a autant (c'est-à-dire $m = m'$).

On voit que p_1 divise $q_1 \cdots q_{m'}$. Par le lemme d'Euclide, p_1 divise un des q_i. Sans nuire à la généralité, on peut supposer que p_1 divise q_1. Par la remarque, on a donc $p_1 = q_1$.

En simplifiant par p_1 l'équation ci-dessus, on trouve

$$p_2 \cdots p_m = q_2 \cdots q_{m'}$$

Sans nuire à la généralité, on montre comme précédemment que $p_2 = q_2$, $p_3 = q_3$, etc. Finalement, il va rester

$$p_m = q_m \cdots q_{m'}$$

Cela signifie en même temps que $p_m = q_m$ et que $m = m'$, car aucun nombre premier n'est égal à 1. □

Remarque

Ce sont les "sans nuire à la généralité" qui sont la cause du mot "essentiellement" qui se trouve dans l'énoncé du théorème fondamental de l'arithmétique.

2.3 Il y a une infinité de nombres premiers

Le théorème fondamental de l'arithmétique nous permet de montrer qu'il existe une infinité de nombres premiers.

2.3.1 Première démonstration

Cette très belle preuve inventée par Euclide, s'est retrouvée dans un poème de Brian D. Beasley, adapté de Robert Frost.

Stopping By Woods
on a Snowny Evening
by Robert Frost

Whose woods these are I think I know.
His house is in the village though;
He will not see me stopping here
To watch his woods fill up with snow.

My little horse must think it queer
To stop without a farmhouse near
Between the woods and frozen lake
The darkest evening of the year.

He gives his harness bells a shake
To ask if there is some mistake.
The only other sound's the sweep
Of easy wind and downy flake.

The woods are lovely, dark and deep.
But I have promises to keep,
And miles to go before I sleep,
And miles to go before I sleep.

Stopping by Euclid's Proof
of the Infinitude of Primes
by Brian D. Beasley

Whose proof this is I think I know.
I can't improve upon it, though;
You will not see me trying here
To offer up a better show.

His demonstration is quite clear :
For contradiction, take the mere
n primes (no more), then multiply;
Add one to that...the end is near.

In vain one seeks a prime to try
To split this number — thus, a lie!
The first assumption was a leap;
Instead, the primes will reach the sky.

This proof is lovely, sharp, and deep.
But I have promises to keep,
And tests to grade before I sleep,
And tests to grade before I sleep.

Démonstration d'Euclide

On suppose par l'absurde qu'il y a un nombre fini de nombres premiers, disons n nombres premiers. Dans ce cas, l'ensemble $\mathcal{P}$ s'écrit

$$\mathcal{P} = \{p_1, p_2, p_3, \ldots, p_n\}$$

On examine le nombre

$$N = p_1 \cdot p_2 \cdot p_3 \cdots p_n + 1$$

Comme $N > 1$, il existe, grâce au théorème fondamental de l'arithmétique, un nombre premier p_k (avec $k \in \{1, 2, \ldots, n\}$) qui divise N. Or, ce nombre premier divise aussi $p_1 \cdot p_2 \cdot p_3 \cdots p_n$.

Par conséquent, p_k divise 1 car $1 = n - p_1 \cdot p_2 \cdot p_3 \cdots p_m$. Mais le seul nombre naturel qui divise 1 est 1. De ce fait, on a $p_k = 1$. C'est une contradiction (avec le fait que 1 n'est pas un nombre premier). □

2.3.2 Deuxième démonstration

Cette démonstration a l'élégance de ne pas être une démonstration par l'absurde.

Notation

On note

$$n! = 1 \cdot 2 \cdot 3 \cdots (n-1) \cdot n$$

Par exemple, $1! = 1$; $2! = 1 \cdot 2 = 2$; $3! = 1 \cdot 2 \cdot 3 = 6$.

Théorème

Il existe une infinité de nombres premiers.

Preuve

Il suffit de démontrer que, pour tout nombre entier $n \geqslant 3$, il existe un nombre premier entre n et $n!$.

En effet, si c'est le cas, on sait qu'il y a un nombre premier entre 3 et 3!, un autre entre 3! et (3!)!, encore un autre entre (3!)! et ((3!)!)!, etc.

Montrons donc cette affirmation :

Dans ce but, on considère le nombre $n! - 1$. Puisque $n \geqslant 3$, on a $n! - 1 > 1$.

Par conséquent, ce nombre s'écrit de manière essentiellement unique comme produit de nombres premiers (grâce au théorème fondamental de l'arithmétique). On peut donc prendre un nombre premier p qui divise $n! - 1$.

Montrons par l'absurde que ce nombre premier p satisfait : $p > n$.

> Par l'absurde, on suppose que $p \leqslant n$. Dans ce cas p divise $n! = 1 \cdots p \cdots n$.
>
> Par conséquent, comme p divise $n!$ et $n! - 1$, p divise leur différence qui vaut 1. Or le seul nombre entier positif qui divise 1 est 1 lui-même. Cela voudrait dire que $p = 1$. C'est impossible, car 1 n'est pas premier.

Ainsi p est un nombre premier entre n et $n!$ (en effet, puisque p divise $n! - 1$, on a $p \leqslant n! - 1 < n!$ et on vient de montrer que $p > n$). □