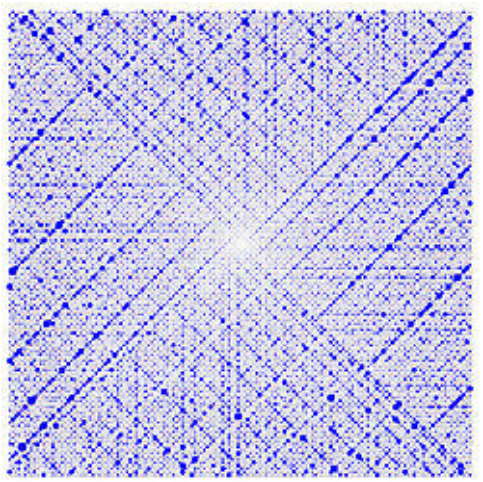
Comment dériver des nombres ?

Partie I - Décomposition en facteurs premiers



Nous aurons besoin pour construire une dérivée sur les nombres d'un résultat d'arithmétique sur les nombres entiers. Ce résultat fait intervenir les nombres premiers.

1. Nombres premiers

On commence par quelques définitions :

Soient a et b deux entiers. La division de a par b consiste à trouver un nombre q (le quotient) et un nombre r (le reste) tels que

$$a = q.b + r, \quad \text{avec} \quad 0 \leq r < b.$$

On dit que b est un *diviseur* de a (ou que a est *multiple* de b) si $r = 0$.

Nous pouvons maintenant donner la définition des nombres premiers :

Définition 1. — *Un nombre supérieur à* 1 *dont les seuls diviseurs sont* 1 *et lui-même est dit premier.*

Un nombre qui n'est pas premier est dit *composé*.

2. Le crible d'Ératosthène

Il n'est pas évident de vérifier qu'un nombre est un nombre premier.

1. Trouver tous les nombres premiers inférieurs à 20.
2. Comment trouver tous ceux inférieurs à 100 ?

Si vous avez eu quelques difficultés avec la question précédente, vous serez sans doute intéressés par une méthode assez simple pour obtenir tous les nombres premiers inférieurs à une certaine borne n donnée, appellée *crible d'Ératosthène*. L'algorithme est le suivant :

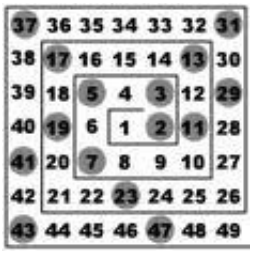
- Écrire tous les entiers de 2 à n;
- Enlever tous les multiples de 2 sauf 2;
- Repérer le premier nombre plus grand que 2 encore présent, c'est à dire 3, et enlever tous les multiples de 3 sauf 3;
- Repérer le premier nombre plus grand que 3 encore présent, c'est à dire 5, et enlever tous les multiples de 5 sauf 5;
- Etc.
- S'arrêter dès qu'on atteint la racine carré de n.

Ce qui reste est la table des nombres premiers jusqu'à n!

1. Pourquoi peut-on s'arrêter à la racine carré de n ?
2. Illustrer le crible d'Ératosthène sur les nombres entiers plus petits que 100 en indiquant les 3 premières étapes.

3. Une représentation géométrique : La spirale d'Ulam

La spirale d'Ulam est une représentation des nombres premiers. On dispose les nombres entiers suivant une spirale de la façon suivante :



et on noircit les nombres premiers. La figure fait apparaître des structures qui contiennent de nombreux nombres premiers (par exemple certaines diagonales) mais dont l'origine est difficile à interpréter. La figure donnée en début de projet correspond à la spirale d'Ulam pour les entiers de 1 à 100000.

4. Le théorème fondamental de l'arithmétique

Cette section sera au coeur de la dérivation sur les nombres. Le théorème que nous allons démontrer est le suivant :

Théorème 1. — *Tout nombre entier supérieur à* 1 *s'écrit de manière unique (à l'ordre près) sous la forme d'un produit de nombres premiers.*

Nous allons démontrer ce résultat en deux étapes : la première concernera l'existence et la seconde l'unicité de la décomposition.

1. Donner des exemples de décomposition de nombres entiers en produit de facteurs premiers.

Vous avez dû remarquer que sans méthode la recherche de cette décomposition est loin d'être évidente. Nous allons donc donner un algorithme de décomposition :

Soit a un nombre entier.

- Tenter toutes les divisions de a par les nombres premiers entre 2 et $\sqrt{a}$.
- Dès qu'un facteur premier p est trouvé, mémoriser p, diviser a par p, et reprendre l'algorithme avec ce nouveau nombre.
- Si aucun diviseur n'est trouvé, c'est que a est premier ; l'ajouter à la liste.

La liste des nombres premiers ainsi constituée est la décomposition du nombre a initial en facteurs premiers.

1. Décomposer 220 et 100 et 65000.
2. Décomposition de 1111111 ?

Vous l'aurez compris avec ce dernier exemple, la décomposition en facteur premier n'est pas simple !

4.1. Un premier résultat. — Le théorème de décomposition est basé sur le petit lemme suivant :

Lemma 1. — *Tout nombre entier supérieur à* 1 *est divisible par un nombre premier.*

La démonstration utilise le principe de récurrence. Il faut d'abord remarquer que ce résultat est vrai pour 2 qui est premier. Nous supposons maintenant que le résultat du lemme est vrai pour tous les entiers compris entre 2 et n.

1. Que peut-il se passer pour $n+1$?

4.2. Existence de la décomposition. — L'existence de la décomposition se fait aussi par récurrence. Le résultat est vrai pour 2. Supposons qu'il soit vrai pour tous les nombres compris entre 2 et n.

Que se passe-t-il pour $n+1$?

Si $n+1$ est premier c'est terminé.

Si $n+1$ n'est pas premier.....

1. Utiliser le lemme précédent !

La démonstration de l'unicité de la décomposition demande plus de travail.