Cours du 12.10.2020 - MATIN
dimanche, 11 octobre 2020 18:15

Rappel: Test le jeudi 29.10.2020

Chapitre 2: Eléments de théorie des nombres

Les premières notions étaient l'étude de triplets de la forme

$a^2 + b^2 = c^2$ (v 1800 av J.-C.)

$3^2 + 4^2 = 5^2$

Questions qui se posent:

- Qu'est-ce qu'un nombre premier?
- Y en a-t-il une infinité ?
- Y a-t-il une formule pour les générer ?

Problèmes "ouverts": (Conjecture)

- Existe-t-il une infinité de premiers "jumeaux" (p est premier et p+2 est premier)

  (5,7); .... ?

- Conjecture de Goldbach: tout entier pair ≥ 4 peut s'écrire comme la somme de 2 premiers.

Conjecture de Fermat (1601-1655)

L'équation $x^n + y^n = z^n$ a-t-elle une solution entière pour tout n ?

Réponse: non si $n \geq 3$

Preuve: "il existe une magnifique preuve à ce problème, mais la marge est trop petite pour la contenir."

Dernier théorème de Wiles-Fermat, qui a prouvé par Andrew Wiles 1995.

Nombres Premiers :

P est premier si il est divisible par 1 et par lui-même.

⚠ 1 n'est PAS premier.

Q : 1) Y en a-t-il une infinité ? OUI (par l'absurde)

2) Existe-t-il un générateur / formule pour les trouver ? NON

Il faut tester si un nombre est premier ou non !

↳ Si N n'est PAS premier alors il existe $x, y \in \mathbb{N}$ tels que $N = x \cdot y$ $\quad x, y \in [2, \dots, N-1]$

Algorithme simple :

pour $i = 2, \dots, N-2$

Si $N \% i == 0 \Rightarrow$ i divise N, N PAS premier STOP.

$i++;$

Si $i = N-2 \rightarrow$ N est PREMIER...

Algo est de complexité $O(N)$ (linéaire)

SIMPLE ⟶ COMPLEXE

$O(1)$ → temps constant (Accès à un élément dans une HASH-map)

$O(\log(N))$ Binary search (Dicotomie)

$O(N)$ linéaire (N premier)

$O(N^2) \dots O(\text{polynôme}(N))$ complexité polynômiale

$O(c^N) \rightarrow O(N^N)$ problèmes exponentiels

← FACILES | DIFFICILE →

Peut-on faire mieux pour tester si N est premier ?

oui : $O(\sqrt{N})$ Pourquoi : ...

oui : $O(\sqrt{N})$

pourquoi : si $N = x \cdot y$

si $x = y$ alors $x = y = \sqrt{N}$ $(N = x^2 = y^2)$

Sinon l'un est plus grand que l'autre

$x < y$

$1 < x < \sqrt{N}$ et $\sqrt{N} < y < N$

$\Rightarrow$ Si N n'a PAS de diviseur entre $]1, \sqrt{N}]$, il n'en a pas non plus dans $[\sqrt{N}, N[$! $\Rightarrow$ N est premier s'il n'a AUCUN diviseur de $[2, \dots, \sqrt{N}]$

$N \longmapsto$ premier oui ou non ? $O(\sqrt{N})$ (Facile)

$N \longmapsto$ Quelle est la liste des premiers $\leq N$?

Crible d'Eratosthène :

1) Ecrire les nombres de $2 \dots N$
2) Entourer (2) et biffer tous les multiples de 2
3) Entourer le prochain élément non biffé (c'est un premier) biffer tous ses multiples !

STOP à 5 car $7 > \sqrt{30} = 5,\dots$

Tous je peux m'arrêter à 5, tout ce qui reste sera premier !!!

$O(n\sqrt{n})$

Théorème Fondamental de l'arithmétique: Gauss (1777-1855)

Tout nombre entier $N \geq 2$ peut s'écrire comme un produit fini de nombres premier. De façon UNIQUE !

Ce produit s'appelle la FACTORISATION en facteurs premiers

Exemple:

$$924 = 2 \cdot 462 = 2 \cdot 2 \cdot 231 = 2 \cdot 2 \cdot 3 \cdot 7 \cdot 11$$