

TEST jeudi 29.10.2020

Chapitre 2: Théorie des Nombres



Début de l'étude des nombres ~ 1800 Av. J.-C.

$$a^2 + b^2 = c^2$$

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

l'étude des triplets de cette forme
Nombres ENTIERES

Étude des Nombres premiers:

P est premier s'il n'est divisible que par 1 et lui-même!
entière

1 est-il premier? NON!

- Y a-t-il une infinité de premiers? OUI prouvé par l'absurde
- On n'a pas encore trouvé de formule pour générer des nombres premiers...

Problèmes ouverts:

- Existe-t-il une infinité de premiers "jumeaux"
 p et $p+2$ premiers $(3, 5; 5, 7; 11, 13; 29, 31, \dots)$
- Conjecture de Goldbach: tout entier PAIR ≥ 4 peut s'écrire comme la somme de 2 premiers.

Conjecture de Fermat (1601-1655):

L'équation $a^n + b^n = c^n$ n'a pas de solution ENTIERE pour $n \geq 3$!

"Il existe une preuve remarquable à ce théorème, mais la marge est trop petite pour la contenir"

"Il existe une preuve remarquable à ce théorème, mais la marge est trop petite pour la contenir"

1995 cela devient le Théorème de Wiles-Fermat.

Comment vérifier si N est premier ?

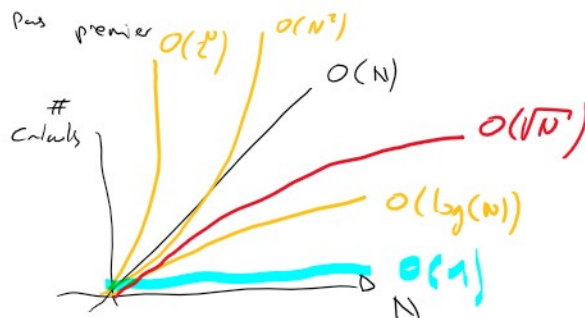
Si $N = 1 \Rightarrow$ Non

pour $i = 2 \dots N-1$ $O(N)$

Si $N \% i == 0 \Rightarrow$ Non N est divisible par i
 $\Rightarrow$ Pas premier
 STOP

Sinon $i = i + 1$

Q. signifie $O(N)$
 $\downarrow$
 ORDRE de complexité



$O(N) \Rightarrow$ le nombre de calculs
 est $\approx C \cdot N$
 $\uparrow$
 constante

Simple $\longrightarrow$ Complexe $\xrightarrow{\text{constant}}$
 $O(1) - O(\log(N)) - O(N) - O(N^2) - O(N^3) \dots O(P^N)$
 temps constant linéaire polynomial exponentiel
 "FACILE"

Pour-on faire mieux pour vérifier si N est premier ?

Oui :

Si N PAS premier $N = x \cdot y$

x, y entiers entre $[2 \text{ et } N-1]$

Si $x = y$ alors $x^2 = y^2 = N \Rightarrow x = y = \sqrt{N}$

Sinon alors $x > y$ (l'un est plus grand, supposons que c'est x)

y x



$$\Rightarrow y \in [2, \sqrt{N}] \text{ et } x \in [\sqrt{N}, N-1]$$

$\Rightarrow$ pour prouver que N est premier, il suffit de montrer qu'il n'a pas de diviseurs de 2 à $\sqrt{N}$!

$\Rightarrow$ tester si N est premier $O(\sqrt{N})$