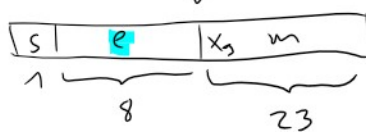


ANNONCE: Test le 9.11.2020

Récap:

- Un nombre s'écrit dans une base $()_b$
- $(x_4 x_3 x_2 x_1 x_0)_b = x_4 \cdot b^4 + x_3 \cdot b^3 + \dots$ $()_b \rightarrow ()_{10}$
- $()_{10} \rightarrow ()_b$: $\begin{cases} \text{Méth. Soustraction} \\ \text{Méth. Division} \end{cases}$
- Pour les nombres Négatifs (entiers) Complément à base 2
 $()_{2^N}$ (méthode d'inversion des bits)
 $()_{10} \rightarrow ()_{2^N}$
- Ecriture scientifique en base b
 $(x_4 x_3 x_2 x_1 x_0, x_{-1} x_{-2} x_{-3})_b = \dots x_i \cdot b^2 + x_i \cdot b + x_0 \cdot 1 + x_{-1} \cdot b^{-1} + \dots$
 Rappel: $b^{-1} = \frac{1}{b}$

- IEEE 754 pour les nombres à virg. flottante



bit caché

$$(X)_{10} = (-1)^s \cdot 2^{e-127} + ((1) + x_9 \cdot 2^{-1} + x_{10} \cdot 2^{-2} + \dots)$$

Δ Ecriture dénormalisée

Si $e=0$ alors le bit caché est 0!

$$()_{10} \rightarrow ()_{IEEE}$$



$$(-1)^s (X, Y)_{10} \mapsto (-1)^s (A, B)_2 \neq (1, AB)_2 \cdot 2^E \xrightarrow{\quad} (E+127)_{10} \xrightarrow{\quad} ()_2$$

$$\boxed{s \mid e \mid m}$$

$$()_{EEEE} \mapsto ()_{10} = (-1)^s \cdot 2^{(e-127)} \cdot (1, m)_2 \left(\sim (-1)^s \pi \cdot 2^{(e-127)/3.3} \right)$$

$$\Downarrow$$

$$\pi = ()_{10}$$

Chapitre 2: Éléments de la théorie des nombres ($\mathbb{N}$)

Les premières notions remontent à ~ 1800 av. J.-C.

quels sont les triplets du type $a^2 + b^2 = c^2$

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

Questions Types:

- y a-t-il une infinité de ces triplets? OUI! il y a une infinité de triangles rectangles!
- qu'est-ce qu'un nombre premier? (divisible uniquement par 1 et lui-même)
- y en a-t-il une infinité? OUI (Preuve par l'absurde)
- y a-t-il une formule? (on en connaît pas!)

Conjectures: (problèmes ouverts)

- Existe-t-il une infinité de premiers jumeaux

$$(p, p+2) \quad [3, 5], [5, 7], \dots, [29, 31], \dots$$

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

Conjecture de Fermat (1601-1657)

Conjecture de Fermat (1601 - 1655)

L'équation $x^n + y^n = z^n$ a-t-elle une solution entière. ^{$(x, y, z \in \mathbb{N})$}

Oui pour $n \leq 2$, Non pour $n \geq 3$!

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

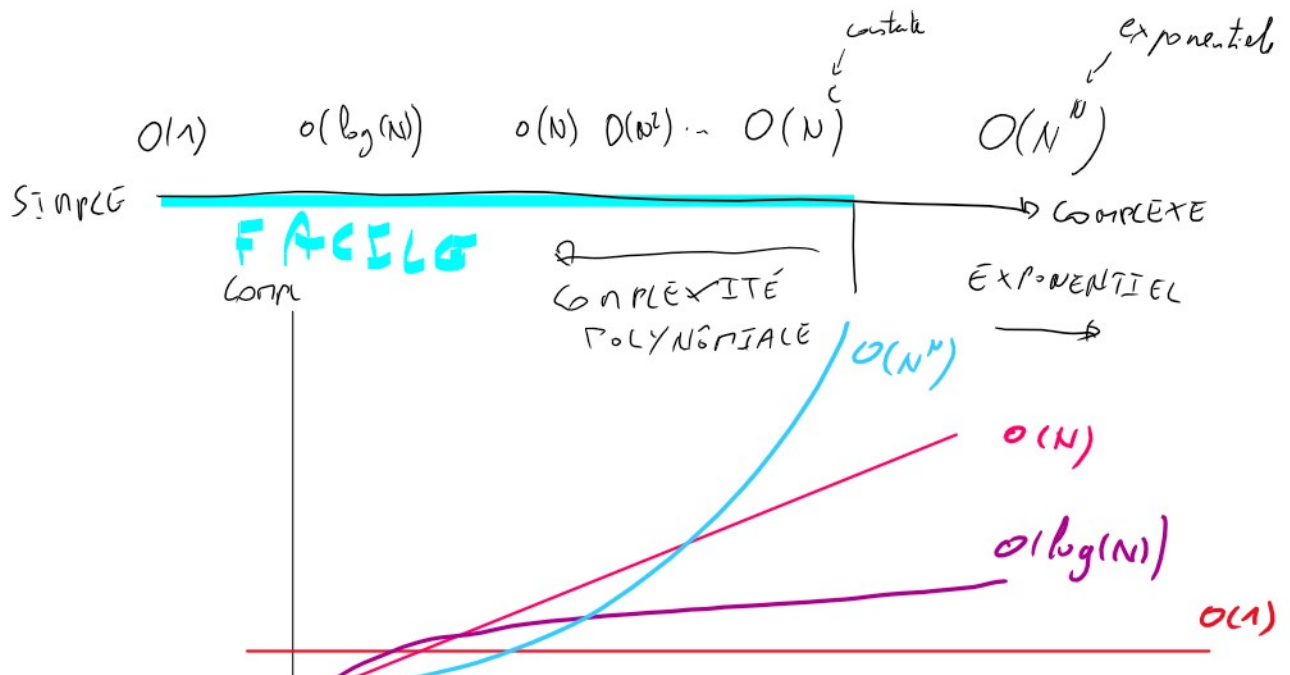
Devenu Théorème de Wiles Fermat 1995... Preuve fait plus 1000 pages!

Comment on teste si $N \in \mathbb{N} \setminus \{0, 1\}$ est premier?

$\sim n$ test $\left(\begin{array}{l} \text{for } i = 2, \dots, N-1 \\ \quad \text{Si } N \bmod i == 0 \Rightarrow \text{STOP PAS PREMIER} \\ \text{end} \\ \Rightarrow \text{si on arrive ici, } N \text{ est premier} \end{array} \right.$

$O(N)$ complexité d'ordre N

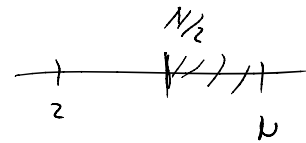
calculs $c \cdot N$ où c const.



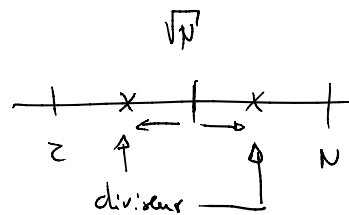


On peut faire mieux: il suffit de voir que si N n'est PAS premier, il a au moins 2 diviseurs

$$N = a \times b \quad a, b \in [2, \dots, \frac{N}{2}]$$



Plus grand diviseur possible est $\sqrt{N}$



Si N n'est PAS premier, il y a forcément

un diviseur dans $[2, \sqrt{N}] \Rightarrow$ il suffit de faire $\sqrt{N}$ tests.

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

Comment créer une liste de nombres premiers de $1, \dots, N$?

Crible d'Eratosthène:

- 1) Ecrire tous les nombres de $2, \dots, N$
- 2) Entourer le plus petit nombre non-biffé,
- 3) Biffer tous les multiples du nombre entouré,
revenir au 2) ...

3) Biffe les multiples du nombre entouré,

relance au pt 2) jusqu'à avoir dépassé $\sqrt{N}$

	<u>2</u>	<u>3</u>	4	<u>5</u>	6	<u>7</u>	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

$\sqrt{N} = \sqrt{100} = 10$
Stop

Ceux qui restent sont premiers!

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

Tout nombre entier $N \geq 2$ peut s'écrire comme le produit fini de nombres premiers. De plus, l'écriture est UNIQUE à l'ordre près!

On appelle cette écriture la "FACTORISATION" (ou la "DÉCOMPOSITION") de N en facteurs premiers!

⚠ 1 n'est PAS premier (sinon la factorisation ne serait pas unique!)

Exemple: $154 = 2 \cdot 7 \cdot 11$

$$3 = \underline{3} (x 1)$$

Q:1 Comment trouver la factorisation de N ?

Brute Force: on divise N par le plus petit premier non-testé

Brute Force:

on divise N par le plus petit premier non-testé
tant que c'est possible.

on passe au premier suivant et on recommence !

Factorisation 770:

~~2~~, ~~3~~, ~~5~~, ~~7~~, ~~11~~, 13, 17, 19, 23

$$770 = 2 \times 385$$

$$770 = 2 \times 5 \times 7 \times 11$$

$$385 = 5 \times 77$$

$$77 = 7 \times 11$$

Factoriser 168:

~~2~~, ~~3~~, ~~5~~, ~~7~~, 11

$$168 = 2 \times 84$$

$$84 = 2 \times 42$$

$$42 = 2 \times 21$$

$$21 = 3 \times 7$$

$$7 = 7 \times 1$$

$$168 = 2 \times 2 \times 2 \times 3 \times 7$$

$$= 2^3 \times 3 \times 7$$