Nombres Premiers

Anca Nitulescu
anca.nitulescu@ens.fr

Ecole Normale Supérieure, Paris

5 octobre 2016

Primalité

Définition

Un nombre p est premier si ses seuls diviseurs positifs sont p et 1.

Liste : $2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29,\ \ldots$

Propriétés

- Entre n et $2n$, il y a toujours un nombre premier.
- Un nombre pair est toujours la somme de 2 premiers.
- Un nombre impair (>5) est la somme de 3 premiers.

Théorème d'Euclide

Il existe une infinité de nombres premiers.

Décomposition en facteurs prémiers

Théorème fondamental de l'arithmétique

Tout entier **n** s'écrit de façon unique comme produit de puissances de nombres premiers :

$$n = \prod_{i=1}^{k} p_i^{\alpha_i}$$

PGCD

Si $a = \prod_i p_i^{\alpha_i}$ et $b = \prod_i p_i^{\beta_i}$, alors :

$$\mathrm{pgcd}(a, b) = \prod_i p_i^{\min(\alpha_i, \beta_i)}$$

Théorème Gauss

Si p est premier et $p|ab$ alors $p|a$ ou $p|b$.

Distribution des nombres premiers

Question

Il existe une infinité de nombres premiers. (Euclide)

Comment sont-ils *répartis* ? ? ?

1	**2**	**3**	4	**5**	6	**7**	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

Théorème des nombres premiers

Soit $\pi(n)$ le nombre de nombre premiers inférieurs ou égaux à n.

$$\pi(n) \sim \int_2^n \frac{dx}{\ln n} \sim \frac{n}{\ln n} + \frac{n}{(\ln n)^2} + \frac{2n}{(\ln n)^3} + \dots$$

Distribution des nombres premiers

En pratique

Le nombre de premiers inférieurs à n est de l'ordre de $n/\ln n$.

Conclusions :

- il y a environ 2^{1014} nombres premiers de 1024 bits
- la probabilité qu'un nombre x soit premier est proche de $1/\ln n$,
- probabilité de $1/710$ pour un entier de 1024 bits