Extrait de Pour la Science n° 251 Septembre 1998 :

La factorisation des grands nombres (Johannes Buchmann)

Le nombre 114 381 625 757 888 867 669 235 779 976 146 612 010 218 296 721 242 362 562 561 842 935 706 935 245 733 897 830 597 123 563 958 705 058 989 075 147 599 290 026 879 543 541 est le produit de deux nombres premiers ; lesquels ?

Martin Gardner posa cette question aux lecteurs de Pour la Science en octobre 1977. dans sa rubrique de «Jeux mathématiques», mais une réponse ne fut donnée que 16 ans plus tard : en avril 1994, Paul Leyland, de l'Université d'Oxford. Michael Graff, de l'Université de l'lowa, et Derek Atkins, de l'Institut de technologie du Massachusetts, identifièrent les deux facteurs, après avoir distribué des parties de la tâche, grâce au réseau Internet, à quelque 600 volontaires, qui laissèrent fonctionner sur leurs ordinateurs, pendant de nombreuses nuits, le programme écrit par Arjen Lenstra, du Centre de recherches de la Société Bell Communications.

La multiplication de deux nombres, même très grands, n'est pas compliquée : avec du papier et un crayon, on calcule le produit de deux nombres de 65 chiffres en une heure environ ; par ordinateur, le calcul est immédiat. En revanche, l'opération inverse, c'est-à-dire l'identification des facteurs d'un produit, est très difficile, même avec les calculateurs les plus rapides. (...)

Les opérations mathématiques telles que la multiplication et la factorisation sont à la base des systèmes cryptographiques modernes : le cryptage est rapide, mais le décryptage est quasi impossible en pratique. (...)

On ignore si la factorisation est difficile par essence ou si les mathématiciens n'ont pas encore trouvé la méthode la plus habile. Aussi la seule garantie de la sécurité des procédés de cryptage est l'ignorance d'une méthode rapide de factorisation des nombres entiers. L'étude de la factorisation date de l'antiquité : les mathématiciens d'alors savaient déjà que chaque nombre naturel est un produit de nombres premiers, et que la décomposition en facteurs premiers est unique, à l'ordre près. Par exemple, 12 se décompose seulement en $2 \times 2 \times 3$. L'étude des propriétés des nombres entiers naturels impose souvent la décomposition en facteurs premiers. (...)

1. Notion de nombres premiers

Définition : Soit p un entier naturel strictement supérieur à 1. On dit que p est un nombre premier si l'ensemble de ses diviseurs dans $\mathbb{N}$ est $\{1 ; p\}$.

Exemple : 2 ; 3 ; 5 ; 7 sont des nombres premiers. 4, 6, 8, 9, 10 ne sont pas des nombres premiers.
Par convention, et pour des raisons de facilité, 1 n'est pas un nombre premier.

Propriétés :
Soit a un entier naturel strictement supérieur à 1.
- a possède au moins un diviseur premier.
- si a n'est pas premier, alors au moins un des diviseurs premiers de a est inférieur ou égal à $\sqrt{a}$.

Remarque : Test de primalité :
Pour déterminer si un nombre donné N est premier, on peut chercher s'il est divisible par un nombre premier inférieur ou égal à $\sqrt{N}$.
- Si l'un des nombres premiers inférieurs ou égaux à $\sqrt{N}$ divise N, alors N n'est pas premier.
- Si aucun des nombres premiers inférieurs ou égaux à $\sqrt{N}$ ne divise N, alors N est premier.

Cette méthode nécessite de connaître la liste des nombres premiers inférieurs ou égaux à $\sqrt{N}$.

Un entier naturel strictement supérieur à 1 et qui n'est pas premier est appelé nombre composé.

2. Crible d'Eratosthène

Le crible d'Eratosthène est une méthode permettant d'obtenir tous les nombres premiers inférieurs à un nombre donné. Pour trouver par exemple tous les nombres premiers inférieurs à 100, on écrit dans un tableau tous les nombres de 1 à 100.

On raye le nombre 1 qui n'est pas premier. Le premier nombre non rayé est 2, il est premier.
On raye tous les multiples de 2 supérieurs à 2. Le premier nombre non rayé est 3, il est premier.
On raye tous les multiples de 3 supérieurs à 3. Le premier nombre non rayé est 5, il est premier.
On raye tous les multiples de 5 supérieurs à 5. Le premier nombre non rayé est 7, il est premier.
On raye tous les multiples de 7 supérieurs à 7. Le premier nombre non rayé est 11, il est premier.
On peut s'arrêter car $11 > \sqrt{100}$.
On a obtenu alors dans les cases non rayées, les nombres premiers inférieurs à 100.
Les nombres rayés ne sont pas premiers puisque ce sont des multiples de l'un des nombres qui précèdent.
Si un nombre N n'est pas rayé, c'est que N n'est multiple d'aucun des nombres non rayés strictement inférieurs à 11, donc N n'est multiple d'aucun nombre premier strictement inférieur à $\sqrt{N}$, donc N est premier.

Propriété : Il existe dans $\mathbb{N}$ une infinité de nombres premiers.

3. Décomposition d'un nombre en produit de facteurs premiers

Propriété : Soit n un entier supérieur ou égal à 2. Le nombre n peut se décomposer sous la forme :
$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times p_3^{\alpha_3} \times ... \times p_n^{\alpha_n}$ où les p_i (i variant de 1 à n) sont des nombres premiers tels que $p_1 < p_2 < p_3 < ... < p_n$ et les α_i (i variant de 1 à n) sont des entiers naturels non nuls.
Cette décomposition est appelée décomposition de n en produit de facteurs premiers.
On admet que cette décomposition est unique.

Remarque : Du fait de l'unicité de la décomposition, si $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times p_3^{\alpha_3} \times ... \times p_n^{\alpha_n}$, alors tout diviseur premier de n est l'un des p_i (i variant de 1 à n).

Exemple : Décomposition d'un nombre en produit de facteurs premiers : On considère le nombre 360.
Il est divisible par 2 et on peut écrire $360 = 2 \times 180$
180 est encore divisible par 2 et on peut écrire $180 = 2 \times 90$
90 est encore divisible par 2 et on peut écrire $90 = 2 \times 45$
45 est divisible par 3 et on peut écrire $45 = 3 \times 15$
15 est divisible par 3 et on peut écrire $15 = 3 \times 5$
Finalement on obtient $360 = 2 \times 2 \times 2 \times 3 \times 3 \times 5 = 2^3 \times 3^2 \times 5$.
C'est la décomposition du nombre 360 en produit de facteurs premiers.

Certaines calculatrices et certains outils de calcul sur ordinateur permettent d'obtenir la décomposition d'un nombre en produit de facteurs premiers :

Propriété : Un naturel d divise un entier naturel n si et seulement si les facteurs premiers de la décomposition en facteurs premiers de d se trouvent dans celle de n avec des exposants au moins égaux à ceux avec lesquels ils figurent dans celle de d.
C'est-à-dire si $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times p_3^{\alpha_3} \times ... \times p_n^{\alpha_n}$, alors $d = p_1^{\beta_1} \times p_2^{\beta_2} \times p_3^{\beta_3} \times ... \times p_n^{\beta_n}$, où les $0 \leqslant \beta_i \leqslant \alpha_i$.

Recherche des nombres premiers de 1 à 300 à l'aide du crible d'Erathostène:

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
101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128	129	130	131	132	133	134	135	136	137	138	139	140
141	142	143	144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159	160
161	162	163	164	165	166	167	168	169	170	171	172	173	174	175	176	177	178	179	180
181	182	183	184	185	186	187	188	189	190	191	192	193	194	195	196	197	198	199	200
201	202	203	204	205	206	207	208	209	210	211	212	213	214	215	216	217	218	219	220
221	222	223	224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239	240
241	242	243	244	245	246	247	248	249	250	251	252	253	254	255	256	257	258	259	260
261	262	263	264	265	266	267	268	269	270	271	272	273	274	275	276	277	278	279	280
281	282	283	284	285	286	287	288	289	290	291	292	293	294	295	296	297	298	299	300

Quelques critères de divisibilité:

Un nombre entier est divisible par 2 si son chiffre des unités est pair.
Un nombre entier est divisible par 3 si la somme de ses chiffres est divisible par 3.
Un nombre entier est divisible par 5 si son chiffre des unités est 0 ou 5.
Un nombre entier est divisible par 7 si $d + 5u$ (le nombre étant $10\,d + u$) est divisible par 7.
Un nombre entier est divisible par 9 si la somme de ses chiffres est divisible par 9.
Un nombre entier est divisible par 10 si la somme de ses chiffres est divisible par 3.
Un nombre entier est divisible par 11 si la différence entre la somme des chiffres de rang pair et la somme des chiffres de rang impair est divisible par 11.