TESTER SI UN NOMBRE EST PREMIER

Notions réinvesties : petit théorème de Fermat, congruences

Un nombre étant donné, comment savoir le plus rapidement possible s'il est premier ?
Sinon, quelle est sa décomposition en facteurs premiers ?

La question est facile pour les petits nombres : il suffit d'utiliser naïvement la définition de la primalité et de tester tous les diviseurs possibles avec un ordinateur. En revanche, dès qu'on traite de grands nombres (à partir de 20 chiffres), la question se révèle très délicate, encore davantage pour la factorisation.

Ce sujet étant intimement lié à la cryptographie numérique moderne (comme le système R.S.A.), dont les enjeux politiques et économiques sont importants, un effort considérable a été entrepris de toutes parts, et de nouvelles méthodes donnent aujourd'hui à un micro-ordinateur assez de puissance pour déterminer si un nombre de 1 000 chiffres est premier, problème qu'on imaginait inaccessible autrefois.

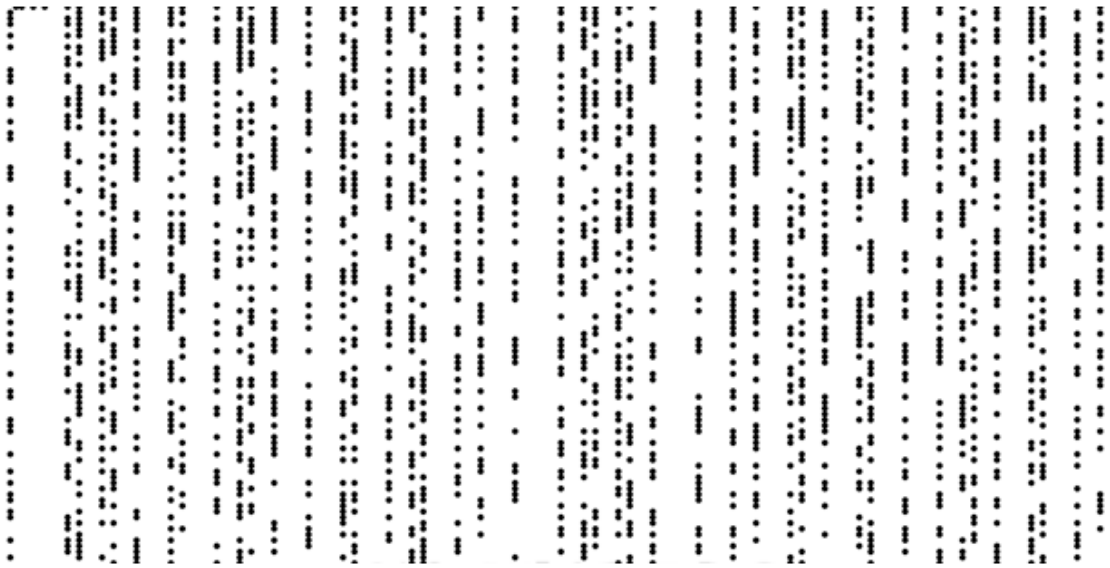
Du fait de leur utilisation dans les algorithmes utilisés pour coder et protéger des données confidentielles, les nombres premiers peuvent faire partie des outils mis à la disposition des entreprises.
Ainsi, le mathématicien Roger Schlafly a déposé en 1994 un brevet commercial sur les deux nombres premiers ci-dessous, exprimés en hexadécimal. Dans cette base, les symboles utilisés sont les chiffres de 0 à 9 puis les lettres A, B, C, D, E et F pour désigner respectivement 10, 11, 12, 13, 14 et 15. Par exemple $\overline{9\mathrm{E}7\mathrm{D}4}^{16}$ *est le nombre* $9\times16^4+14\times16^3+7\times16^2+13\times16+4$ *c'est-à-dire* $649\,172$ *en décimal.*

98A3DF52AEAE9799325CB258D767EBD1F4630E9B9E21732A4AFB1624BA6DF911466AD8DA960586F4A0D5E3C36AF09
9660BDDC1577E54A9F402334433ACB14BCB

93E8965DAFD9DFECFD00B466B68F90EA68AF5DC9FED915278D1B3A137471E65596C37FED0C7829FF8F8331F81A270
0438ECDCC09447DC397C685F397294F722BCC484AEDF28BED25AAAB35D35A65DB1FD62C9D7BA55844FEB1F9401E6
71340933EE43C54E4DC459400D7AD61248B83A2624835B31FFF2D9595A5B90B276E44F9

Un ***nombre premier*** est un entier naturel qui admet exactement deux diviseurs : 1 et lui-même.

Pour déterminer si un entier n est premier, il suffit donc de tester si k divise n, pour tous les entiers k inférieurs à n. Mais si n est très grand, cela peut-être extrêmement long…
Heureusement, d'autres méthodes existent.



Create a table with 180 columns and write down positive integers from 1 in increasing order from left to right, top to bottom. When we mark the prime numbers on this table, we obtain the linear pattern as shown in the figure. [Iris Yoon]

A. Le crible d'Ératosthène

~~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~~

Cet algorithme a été mis au point par Ératosthène (276-194 avant J.-C.), mathématicien grec aussi connu pour ses fonctions de conservateur à la bibliothèque d'Alexandrie, poète, historien, géographe, astronome (il fut le premier à mettre en évidence la rotondité de la Terre) et athlète.

L'algorithme procède par élimination : il s'agit de supprimer d'une table des entiers de 2 à N tous les multiples d'un entier. En supprimant tous les multiples, à la fin il ne restera que les entiers qui ne sont multiples d'aucun entier, et qui sont donc les nombres premiers.

Utilisons cet algorithme pour déterminer
les nombres premiers inférieurs à 100.

On barre 1 car il n'est pas premier.

On ne barre pas 2, qui est premier.
Mais on barre alors tous les multiples de 2 (autres que 2). Pourquoi ?

Le premier nombre non barré est alors 3, qui est premier.
On barre donc tous les multiples de 3 (autres que 3).

Procéder de même avec 5 puis avec 7.

1. Le prochain nombre non barré est alors 11. Pourquoi peut-on s'arrêter ?

2. Pour dresser la liste des nombres premiers inférieurs ou égaux à 1000, jusqu'à quel nombre premier p faudrait-il barrer les multiples ?

3. Lors de l'algorithme, pour éliminer les multiples de a, à quel nombre peut-on commencer ?

Pour visualiser la crible d'Ératosthène jusqu'à 120, voir ici :
https://upload.wikimedia.org/wikipedia/commons/8/8c/New_Animation_Sieve_of_Eratosthenes.gif

B. TEST DE PRIMALITÉ : UN CRITÈRE D'ARRÊT

Soit n un entier naturel non premier tel que $n \geqslant 2$.

On note E l'ensemble des diviseurs positifs de n, autres que 1 et n.

1. Démontrer que E est non vide.
En déduire que E admet un plus petit élément, noté p.

2. Démontrer que p est premier. Quel théorème vient-on de démontrer ?

3. L'entier n s'écrit donc $n = pq$ où $p \leqslant q$.
En déduire que : $p \leqslant \sqrt{n}$.

4. Conclure en écrivant un test de primalité :

TEST DE PRIMALITÉ : CRITÈRE D'ARRÊT

C. TESTS DE FERMAT

Le « petit » théorème de Fermat indique que si p est premier et ne divise pas a, alors $a^{n-1} \equiv 1\ [p]$.
Autrement dit :

PETIT THÉORÈME DE FERMAT

Soit p un nombre premier. Pour tout entier a :
Si p ne divise pas a, alors : $a^{p-1} \equiv 1\ [p]$.

Par conséquent, pour en entier p donné, si on trouve un entier a tel que p ne divise pas a mais $a^{p-1} \not\equiv 1\ [p]$, alors c'est que p n'est pas un nombre premier.
En choisissant a entre 2 et $p-1$, on obtient ce qu'on appelle le ***test de non-primalité de Fermat*** :

TEST DE NON-PRIMALITÉ DE FERMAT

Soit p un entier.
S'il existe un entier a compris entre 2 et $p-1$ tel que $a^{p-1} \not\equiv 1\ [p]$,
alors p n'est ***pas premier***.

UN EXEMPLE

On se demande si le nombre $1111\,111\,111\,111$ est premier.

1. Calculer $2^{1\,111\,111\,111\,110}$ modulo $1111\,111\,111\,111$.

2. Que peut-on en déduire ?

LES NOMBRES DE POULET (ou 2-PSEUDO-PREMIERS)

Utilisons le test de Fermat pour 341.

1. Le nombre 341 est-il premier ?

2. Faire le test de Fermat avec $a=2$. Que constate-t-on ?

On dit que 341 est un ***nombre 2-pseudo-premiers***, ou que c'est un ***nombre de Poulet*** (d'après le mathématicien Paul Poulet qui s'intéressa à ces nombres et en calcula un grand nombre dans les années 1920).

3. 341 est-il 3-pseudo-premiers ?

Les nombres 2-pseudo-premiers sont-ils fréquents ?

On sait que si *n* est un nombre 2-pseudo-premier, alors 2^n-1 l'est aussi.
Par conséquent, il existe ***une infinité de nombres 2-pseudo-premiers***.

En 1949, Erdös montra le joli résultat suivant : pour tout entier $k>1$ donnée, il existe une infinité de nombres 2-pseudo-premiers qui sont chacun produit de *k* facteurs premiers distincts.
En 1971, E. Lieuwens généralisa ce résultat en remplaçant le 2 par un *a*.

Un calcul exhaustif montre que, parmi les nombres inférieurs à 25 milliards, il y a 1 091 987 405 nombres premiers, mais seulement 21 853 nombres 2-pseudo-premiers. Autrement dit, si vous choisissez au hasard un nombre *n* inférieur à 25 milliards :

- il vérifiera $2^{n-1} \not\equiv 1\ [n]$ dans 95,64 % des cas
  et on saura qu'il n'est pas premier ;
- il vérifiera $2^{n-1} \equiv 1\ [n]$ dans 4,36 % des cas,
  et ce sera alors un nombre premier dans 99,998 % des cas.

Au total, en testant si un nombre est 2-pseudo-premier (test de Fermat avec $a=2$), on se trompe dans moins de 0,00009 % des cas.

Avec un intervalle plus grand, le risque diminue encore…

En 1989, Su Hee Kim et Carl Pomerance, des universités de Caroline du Sud et de Géorgie, ont mené une étude théorique sur le risque d'erreur quand on considère premier un nombre *n*, pris au hasard entre 2 et *N*, qui passe le test suivant :

TEST PROBABILISTE DE PRIMALITÉ DE FERMAT
Choisir un nombre *a* au hasard entre 2 et $n-1$.
Si $a^{n-1} \equiv 1\ [n]$, on déclare que *n* est premier.

Le risque est inférieur à 0,0000028 % pour $N=10^{100}$.

Autrement dit, si vous choisissez au hasard un nombre *n* de moins de 100 chiffres et que le test probabiliste de Fermat le déclare premier après avoir tiré au hasard un nombre *a*, alors ***la probabilité que n soit effectivement premier est supérieure à 99,9999972 %***.

Le risque est inférieur à 7,2 % pour un nombre *n* de moins de 60 chiffres.
Le risque est inférieur à $3{,}9\times10^{-25}$ % pour un nombre *n* de moins de 200 chiffres.
Le risque est inférieur à $1{,}2\times10^{-121}$ % pour un nombre *n* de moins de 1000 chiffres.
Le risque est inférieur à $1{,}6\times10^{-1329}$ % pour un nombre *n* de moins de 10 000 chiffres.

Le risque de croire premier un nombre composé choisi par le test probabiliste de Fermat cesse d'être notable dès qu'on s'intéresse à des nombres de plus de 100 chiffres.

Pour des nombres plus courts, le risque ne devient acceptable que si l'on répète plusieurs fois le test.

> Il existe d'autres tests probabilistes, le plus connu et utilisé étant le ***test de Miller-Rabin***.
>
> On considère que les tests probabilistes actuels ont une probabilité d'erreur inférieure à la probabilité que le système informatique qui réalise le test commette une erreur (par exemple une erreur de microprocesseur).

LES NOMBRES DE CARMICHAEL (ou PSEUDO-PREMIERS)

Prenons $561 = 3 \times 11 \times 17$, qui n'est donc pas premier.

1. Vérifier que 561 est 2-pseudo-premier (c'est-à-dire un nombre de Poulet).

2. Ce nombre est-il 4-pseudo-premier ? 5-pseudo-premier ?

3. Écrire un algorithme pour tester si 561 est a-pseudo-premier pour a allant de 2 à 560 avec $a \neq 3$, $a \neq 11$, $a \neq 17$ (on ne prend pas ces trois nombres car alors a et 561 ne sont pas premiers entre eux).

Ces nombres sont aujourd'hui nommés ***nombres de Carmichael***, qui les a étudié en 1912 (bien que A. Korselt en ait parlé le premier dans un article de 1899, passé inaperçu). Par définition, ce sont les nombres n qui trompent le test de Fermat pour toutes les valeurs de a pour lesquelles il est envisageable qu'il soit trompé.

> Il y a 7 nombres de Carmichael inférieurs à 10 000 : 561 ; 1105 ; 1729 ; 2465 ; 2821 ; 6601 ; 8911.
> Entre 10 000 et 100 000, on en trouve 9 autres.
> Il en existe 105 212 inférieurs à 10^{15} .

En 1992 (parution en 1994), W. Alford, A. Granville et C. Pomerance ont résolu une énigme qui a préoccupé de nombreux chercheurs : ils ont montré qu'il existe une ***infinité de nombres de Carmichael***, et qu'ils sont tous impairs.

> En revanche, on ignore toujours si, pour tout k fixé, il existe des nombres de Carmichael ayant exactement k facteurs premiers distincts, et s'il existe une infinité de nombres de Carmichael ayant exactement trois facteurs premiers.

LES NOMBRES DE MERSENNE

A ce jour (février 2017), les sept plus grands nombres premiers connus sont :

Nombre	Nombre de chiffres	Année
$2^{77\,232\,917} - 1$	23 249 425	2018
$2^{74\,207\,281} - 1$	22 338 618	2016
$2^{57\,885\,161} - 1$	17 425 170	2013

Nombre	Nombre de chiffres	Année
$2^{43\,112\,609} - 1$	12 978 189	2008
$2^{42\,643\,801} - 1$	12 837 064	2009
$2^{37\,156\,667} - 1$	11 185 272	2008
$2^{32\,582\,657} - 1$	9 808 358	2006

Tous ces records sont de la forme $2^n - 1$. Ce n'est pas un hasard : les grands nombres premiers sont souvent recherchés sous cette forme car il existe un test efficace (le test de primalité de Lucas-Lehmer, voir plus bas) pour déterminer si un tel nombre est premier ou non.

Un premier résultat qui réduit considérablement les possibilités

1. Vérifier que, pour tout entier $n \in \mathbb{N}^*$: $a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + \ldots + a^2 + a + 1)$.

2. En déduire que si n n'est pas premier, alors M_n n'est pas premier.

3. Que donne la contraposée de ce résultat ? ……

Un théorème qui affine et permet de conclure assez rapidement

Pour trouver les nombres premiers de Mersenne, le théorème suivant, dû à Fermat, est très utile :

> Un diviseur premier d'un nombre de Mersenne $M_p = 2^p - 1$ (avec p premier, $p > 2$) est toujours de la forme $2kp + 1$.

Démonstration

Soit p un nombre premier, $p > 2$.
Supposons que M_p admette un diviseur premier d.
On note I l'ensemble des entiers $n \in \mathbb{N}^*$ tels que $2^n \equiv 1$ [d].

1. Justifier que I n'est pas vide puis qu'il admet un plus petit élément p_0 et que $p_0 > 1$.

2. En écrivant la division euclidienne de n par p_0, montrer que p_0 divise tout élément de I.
En déduire que $p = p_0$.

3. Montrer que p_0 divise $d - 1$, puis qu'il existe un entier naturel k tel que $d = 2kp + 1$.

Applications

Grâce à ce théorème, on trouve assez rapidement ceux des nombres de Mersenne M_p qui sont premiers.
Par exemple, pour étudier la primalité de $M_{13} = 2^{13} - 1 = 8191$, il suffit de tester si ce nombre est divisible par un nombre premier de la forme $2 \times 13k + 1$ inférieur à $\sqrt{8191} \approx 90{,}504$.
Les nombres de la forme $26k + 1$ inférieurs à 91 sont 27, 53 et 79.
Seuls 53 et 79 sont premiers. Comme aucun de ces deux nombres ne divise M_{13}, on peut s'arrêter et conclure que M_{13} est premier.
Prenons l'exemple d'un autre nombre de Mersenne, $M_{11} = 2047$.
Avec la même méthode que celle utilisée ci-dessus, tester la primalité de M_{19} et M_{23}.

Test de Lucas-Lehmer

Ce test fut originellement développé par Édouard Lucas en 1878 et amélioré de façon notable par Derrick Henry Lehmer dans les années 1930.
Il permet de déterminer si un nombre de Mersenne donné est premier.

TEST DE LUCAS-LEHMER POUR LES NOMBRES DE MERSENNE

On note (u_n) la suite définie par $u_0 = 4$ et pour tout entier naturel n :

$$u_{n+1} = u_n^2 - 2.$$

Si $n \geqslant 2$, le test permet d'affirmer que :

M_n est premier $\Leftrightarrow$ $u_{n-2} \equiv 0$ [M_n].

1. Utiliser le test de Lucas-Lehmer pour vérifier que le nombre de Mersenne M_5 est premier.

2. Soit $n \geqslant 3$.
L'algorithme suivant, qui est incomplet, doit permettre de vérifier si le nombre de Mersenne M_n est premier, en utilisant le test de Lucas-Lehmer.

Variables :	u, M, n et i sont des entiers naturels
Initialisation :	u prend la valeur 4
Traitement :	Demander un entier n $\geqslant$ 3 M prend la valeur ..... Pour i allant de 1 à ... faire u prend la valeur ... Fin Pour Si M divise u alors afficher « M ..... » sinon afficher « M ..... »

Compléter cet algorithme, et éventuellement le programmer.

M_{67} : une démonstration silencieuse

Au XVII^{e} siècle, le père Mersenne affirma que $2^{67} - 1$ est un nombre premier, ce qu'on crut vrai pendant 250 ans.

Lors d'une réunion de la Société américaine de mathématiques en 1903, Frank Nelson Cole, de l'Université Columbia, était annoncé pour une conférence intitulée « Sur la factorisation des grands nombres ».

Eric Temple Bell, qui assistait à la séance, raconte :
« Cole - qui n'était pas un homme bavard - s'avança vers le tableau, écrivit soigneusement les puissances de 2 jusqu'à la soixante-septième, retira 1 à cette dernière, ce qui donna le monstrueux résultat 147 573 952 589 676 412 927. Puis il gagna une partie propre du tableau et, toujours sans un mot, calcula le produit $193\,707\,721 \times 761\,838\,257\,287$.
[ndlr : environ une heure de calculs]
Les deux résultats coïncidaient. La conjecture de Mersenne, si c'en était une, tombait dans les limbes de la mythologie mathématique. Pour la première fois, une assemblée de la Société américaine de mathématiques applaudit vigoureusement un conférencier. Cole retourna à son siège sans prononcer un seul mot. Personne ne lui posa de questions. »
Plus tard, Cole admit que cette factorisation lui avait pris « trois ans de dimanches ».

Figure centrale de la vie intellectuelle du XVII^{e} siècle, ***Marin Mersenne*** (1588 - 1648) fait ses études chez les oratoriens du Mans, puis chez les jésuites au collège de La Flèche (où étudiera aussi Descartes), avant de prendre l'habit des minimes (ordre qui doit son nom au désir de ses moines d'être les plus humbles des serviteurs de Dieu). Il enseigne la philosophie à Nevers, puis s'établit à Paris.

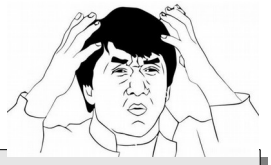
Il y publie divers ouvrages de sciences et de philosophie, dont celui-ci, au titre charmant : *L 'impiété des déistes, athées et libertins, renversée et confondue*. En dépit de cette attaque contre les libres penseurs, il défend la théorie de Galilée contre les critiques théologiques et s'oppose vigoureusement à l'alchimie et à l'astrologie, qu'il dénonce comme pseudosciences.

Le père Mersenne entretient une correspondance avec les plus grands savants de son époque : Descartes, Pascal, Torricelli, Gassendi, Hobbes, Huygens, Roberval, etc. Après sa mort, on trouvera dans ses affaires des lettres de 78 savants.

Il est le premier à utiliser le pendule pour mesurer l'intensité de la pesanteur (qui est, en première approximation, inversement proportionnelle au carré de la période du battement).
Ce touche-à-tout, bien de son époque, conçoit également un hygromètre et un télescope à miroir parabolique, mesure la vitesse du son et découvre la loi des tuyaux sonores et des cordes vibrantes : il comprend ainsi le rapport entre la hauteur des notes de la gamme musicale et la fréquence.

Mersenne s'est bien sûr intéressé aux mathématiques et, notamment, à la primalité des nombres de la forme 2^p-1 . Ces nombres étaient déjà connus d'Euclide, mais ils sont désignés depuis le XVII^{e} siècle sous le nom de nombres de Mersenne, et notés M_p .
L'ecclésiastique français énonce en effet à leur sujet une conjecture qui fera couler beaucoup d'encre: en 1644, il affirme que $M_p=2^p-1$ est un nombre premier pour p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257, et composé pour les autres exposants jusqu'à 257. En 1732, Leonhard Euler pense allonger la liste en affirmant que M_{41} et M_{47} sont des nombres premiers, mais il se trompe. En 1883, I. Pervushin trouve une première erreur dans la liste de Mersenne : il prouve que M_{61} , absent de la liste, est premier. Quatre autres erreurs seront découvertes par la suite : M_{67} et M_{257} ne sont pas premiers, alors que M_{89} et $M_{107,}$ absents de la liste, le sont.

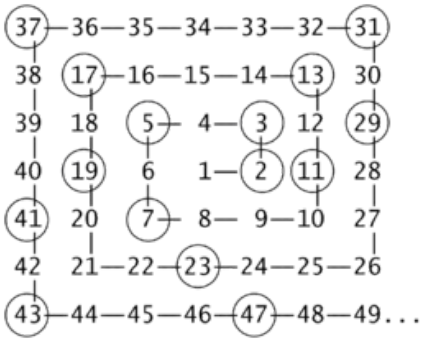
Aujourd'hui, on ignore toujours si, parmi les nombres de Mersenne, une infinité sont premiers.
On ignore également s'il existe une infinité de nombres de Mersenne composés.
Bien sûr, l'une au moins de ces deux affirmations est vraie, probablement les deux.



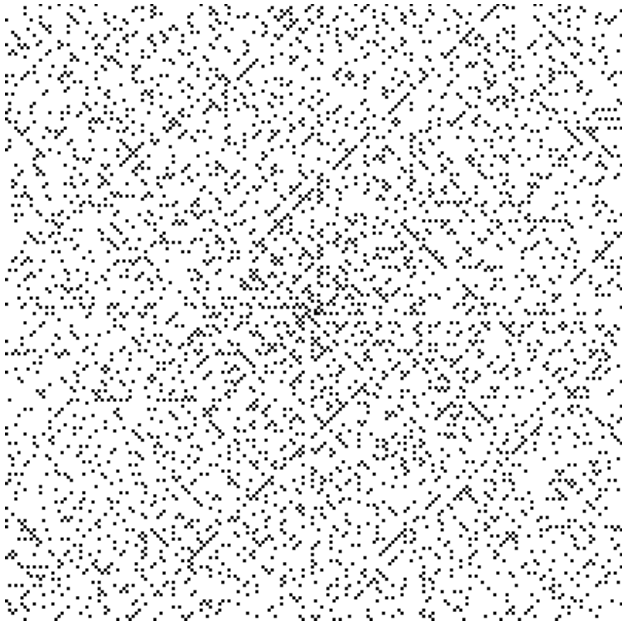
Anecdote

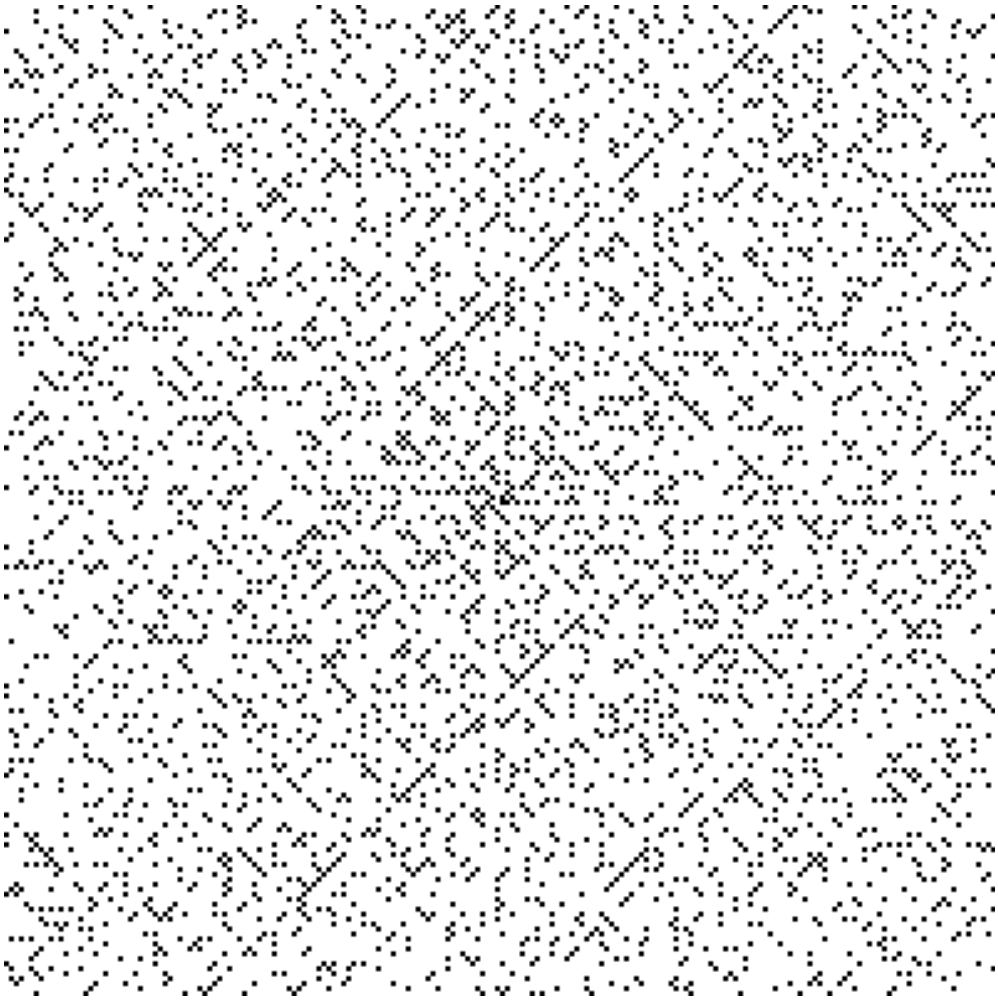
Ronald Graham, des Laboratoires Bell, raconte qu'il a connu un mathématicien qui ne dormait avec son épouse que les jours du mois dont le numéro est un nombre premier : « En début de mois, c'est assez bien - deux, trois, cinq, sept -, mais ça devient plus difficile vers la fin, quand les nombres premiers se raréfient : 19, 23, et le grand saut jusqu'à 29. Ce type était sérieusement frappé. Il est d'ailleurs en prison pour une peine de 20 ans dans le pénitencier de l'Oregon pour kidnapping et tentative de meurtre. »

En mathématiques, la ***spirale d'Ulam*** est une méthode simple pour la représentation des nombres premiers qui révèle un motif qui n'a jamais été pleinement expliqué.
Elle fut découverte par le mathématicien Stanislaw Marcin Ulam, lors d'une conférence scientifique en 1963 : Ulam se trouva coincé, contraint d'écouter « un exposé très long et très ennuyeux ».
Il passa son temps à crayonner et se mit à gribouiller des entiers consécutifs, commençant par 1 au centre, dans une espèce de spirale tournant dans le sens inverse des aiguilles d'une montre. Il obtient une grille régulière de nombres, démarrant par un 1 au centre, et spiralant vers l'extérieur puis entoura tous les nombres premiers, il obtint alors l'image suivante :



À sa surprise, les nombres entourés tendaient à s'aligner le long de lignes diagonales. L'image suivante illustre ceci. C'est une spirale d'Ulam de 200 × 200, où les nombres premiers sont noirs. Les diagonales noires sont clairement visibles.
Ces alignements correspondent à des polynômes du seconde degré du type : $y = a x^2 + b x + c$.





$x^2 + x + 41$

297	296	295	294	293	292	291	290	289	288	287	286	285	284	283	282	**281**
298	237	236	235	234	233	232	231	230	229	228	227	226	225	224	**223**	280
299	238	185	184	183	182	181	180	179	178	177	176	175	174	**173**	222	279
300	239	186	141	140	139	138	137	136	135	134	133	132	**131**	172	221	278
301	240	187	142	105	104	103	102	101	100	99	98	**97**	130	171	220	277
302	241	188	143	106	77	76	75	74	73	72	**71**	96	129	170	219	276
303	242	189	144	107	78	57	56	55	54	**53**	70	95	128	169	218	275
304	243	190	145	108	79	58	45	44	**43**	52	69	94	127	168	217	274
305	244	191	146	109	80	59	46	**41**	42	51	68	93	126	167	216	273
306	245	192	147	110	81	60	**47**	48	49	50	67	92	125	166	215	272
307	246	193	148	111	82	**61**	62	63	64	65	66	91	124	165	214	271
308	247	194	149	112	**83**	84	85	86	87	88	89	90	123	164	213	270
309	248	195	150	**113**	114	115	116	117	118	119	120	121	122	163	212	269
310	249	196	**151**	152	153	154	155	156	157	158	159	160	161	162	211	268
311	250	**197**	198	199	200	201	202	203	204	205	206	207	208	209	210	267
312	**251**	252	253	254	255	256	257	258	259	260	261	262	263	264	265	266
313	314	315	316	317	318	319	320	321	322	323	324	325	326	327	328	329

Sources :

Merveilleux nombres premiers, J.-P. Delahaye, éd. Belin Pour la Science (2ème édition, 2012)
MATH'x, manuel scolaire, éd. Didier, Tle S spécialité (2016)
http://villemin.gerard.free.fr
Wikipedia