L'ESSENTIEL

- Comment déterminer les nombres premiers ? Depuis l'Antiquité, plusieurs formules ont été proposées pour les calculer.
- Certaines sont élégantes, d'autres plus complexes, mais elles ont souvent pour défaut de ne donner que quelques nombres premiers.
- D'autres encore donnent une infinité (théorique) de nombres premiers, mais les valeurs qu'ils prennent croissent trop vite.
- On peut néanmoins s'en inspirer pour faire mieux, notamment en ajustant très finement les paramètres des formules.

L'AUTEUR

SIMON PLOUFFE
professeur à l'IUT Informatique de Nantes, coauteur de l'Encyclopédie en ligne des suites de nombres entiers (OEIS).

Un record pour les nombres premiers

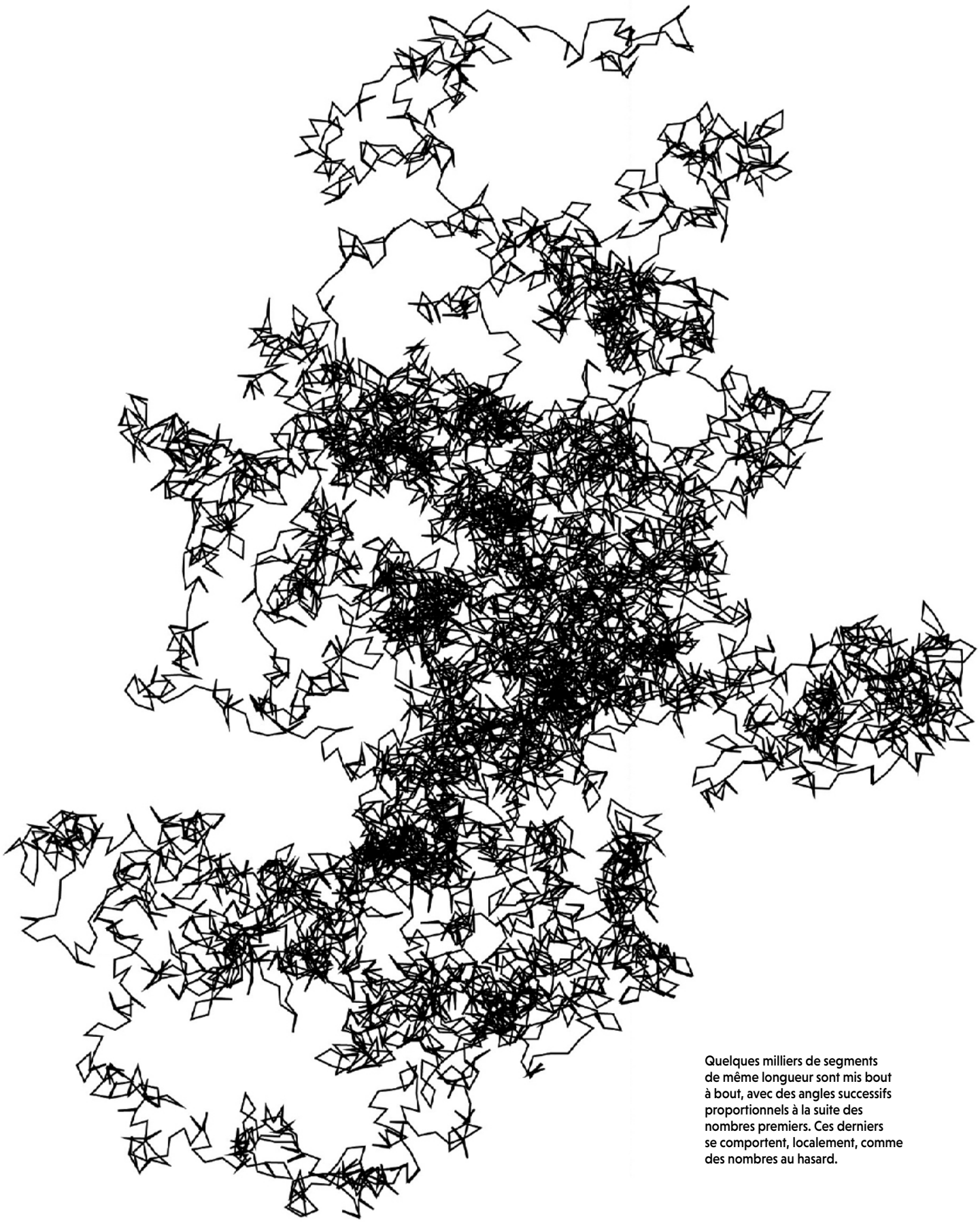
Depuis des millénaires, les mathématiciens conçoivent des formules pour calculer des nombres premiers. En janvier 2019, une formule élaborée par l'auteur a généré une séquence de 100 nombres premiers. C'est un record ! Explications.

Le 7 décembre 2018, un record été battu, celui du plus grand nombre premier connu. $2^{82\,589\,933} - 1$, qui comporte près de 25 millions de chiffres en écriture décimale. On doit cette performance (la vérification est en cours) au *Gimps*, le *Great Internet Mersenne Prime Search*. Ce projet fondé par George Woltman réunit des volontaires mettant à disposition leur ordinateur pour un calcul, distribué, des nombres premiers dits de Mersenne (*voir l'encadré page 79*), c'est-à-dire de la forme $2^p - 1$, p étant un nombre premier. On disposerait donc d'une formule pour déterminer les nombres premiers ?

UNE FORMULE, MAIS LAQUELLE ?

Ce n'est pas aussi simple, notamment parce que tous les nombres premiers ne sont pas de la forme de Mersenne, tant s'en faut. La question se pose donc toujours : y a-t-il une formule pour les nombres premiers ? La réponse est… oui et non.

Et d'abord qu'entend-on par formule ? Par exemple, ce peut être une formule dite close comme celle trouvée par le Suisse Leonhard Euler en 1772 : $p(n) = n^2 + n + 41$. Pour n entre 0 >



Quelques milliers de segments de même longueur sont mis bout à bout, avec des angles successifs proportionnels à la suite des nombres premiers. Ces derniers se comportent, localement, comme des nombres au hasard.

$$\frac{n^6}{72} - \frac{5n^5}{24} - \frac{1493n^4}{72} + \frac{1027n^3}{8} + \frac{100471n^2}{18} - \frac{11971n}{6} - 57347$$

> et 39, elle délivre 40 nombres premiers d'affilée: 41, 43, 47, 53, 61, 71, 83, 97, 113, 131, 151, 173, 197, 223, 251, 281, 313, 347, 383, 421, 461, 503, 547, 593, 641, 691, 743, 797, 853, 911, 971, 1033, 1097, 1163, 1231, 1301, 1373, 1447, 1523 et 1601. De plus, la formule est élégante et simple, mais elle a ses limites. Pour $n = 40$, on trouve 1681... qui est 41^2.

En 2010, François Dress et Bernard Landreau en ont trouvé une meilleure, mais plus compliquée (*voir ci-dessus*). Avec ce polynôme, on obtient des nombres premiers pour n compris entre −42 et 15. La recherche de ce polynôme a tout de même demandé six mois d'efforts avec une batterie d'ordinateurs.

Est-ce donc si difficile de produire une formule qui donnerait quantité de nombres premiers? La question a été close une bonne fois pour toutes en 1947, quand William Mills a publié une formule qui peut donner un nombre arbitraire de nombres premiers. Si A = 1,306377883 8630806904686144926... alors $\lfloor A^{3^n} \rfloor$ donne une suite arbitraire de nombres tous premiers. Ici $\lfloor x \rfloor$ indique que l'on prend la partie entière du nombre x. La suite débute ainsi: 2, 11, 1361, 2521008887... Cependant, les valeurs augmentent très vite, le 8e terme a déjà 762 chiffres, et le 20e environ six milliards!

En 1951, le Britannique Edward Wright en proposait une autre, si $g_0 = \alpha = 1{,}9287800...$ et $g_{n+1} = 2^{g_n}$ alors $\lfloor g_{n+1} \rfloor = \lfloor 2^{...2^{2^\alpha}} \rfloor$ est toujours premier. Les nombres premiers consécutifs sont uniquement représentés par α. La suite obtenue est 3, 13, 16381... le 4e terme a plus de 4932 chiffres et personne n'a osé calculer le 5e...

Ainsi, ces deux suites produisent bien une infinité de nombres premiers, mais le taux de croissance décourage les plus téméraires. Peut-on élaborer des formules fournissant une suite de nombres premiers de longueur arbitraire, mais avec un taux de croissance raisonnable?

Par tous les moyens, on cherche à calculer les nombres premiers, avec une fortune diverse.

Auteur(s)	Année	Commentaire	Efficacité	Nombres calculés
Ératosthène	−276 à −194	Crible d'exclusion	Pratique	Infini calculable
Mersenne	1536	Nombres premiers de la forme 2^p-1.	Pratique, exact	51
Fermat	1640	Petit théorème de Fermat	Produit des premiers probables faibles	Infini calculable
Euler	1772	Polynôme du second degré	Pratique	40
Mills	1947	Double exponentielle	Pratique	Moins de 10
Wright	1951	Super exponentielle	Pratique	Moins de 5
Wilson	vers 1780	Formule qui utilise p!	Théorique	Très peu
Jones, Sato, Wada et Wiens	1976	Polynôme de degré 25 à 26	Théorique	Très peu
John H. Conway	1987	Fractran	Théorique	Très peu
Rowland	2008	Récurrence	Théorique	Très peu
F. Dress et B. Landreau	2010	Polynôme de degré 6	Pratique	58
Benoît Perichon *et al.*	2010	26 premiers en progression arithmétique	Pratique	26
Tomás Oliveira e Silva *et al.*	2019	Programme Primesieve: crible d'Ératosthène optimisé	Le plus rapide connu	Infini calculable sur un ordinateur actuel

LE TABLEAU DE CHASSE

Le «tableau de chasse» ci-contre récapitule des formules et des procédés pour les nombres premiers. L'infini calculable mentionné signifie que le calcul ou procédé peut se dérouler jusqu'à ce que les ressources s'épuisent. Par exemple, le programme Primesieve est le plus rapide. Il peut produire tous les nombres premiers jusqu'à 1000 milliards en 52 minutes sur un ordinateur moyen. Dans sa version courante, la liste peut aller jusqu'à 2^{64}, soit $1{,}844 \times 10^{19}$, mais les nombres réclament 4,1 exaoctets d'espace pour être stockés... Ce programme est fondé sur le crible d'Ératosthène, du nom d'un mathématicien grec du IIIe siècle avant notre ère. Cet algorithme procède par élimination: on supprime parmi les nombres de 2 à N tous les multiples d'un entier de sorte qu'à la fin il ne reste que les nombres premiers.

L'infini calculable du crible d'Ératosthène, à l'époque de son inventeur, était d'un autre ordre, et relevait plus du calcul manuel. La même chose s'applique pour le petit théorème de Fermat selon lequel si p est un nombre premier et si a est un entier non divisible par p, alors $a^{p-1} - 1$ est un multiple de p. Les nombres premiers produits par ce théorème sont probables et faibles. Si p est très grand, il constitue néanmoins un test probabiliste pratique de la primalité d'un nombre candidat.

Quant aux nombres de Mersenne (de la forme $2^p - 1$), ils sont limités par la taille de p. Pour tester un seul exposant dans la liste des candidats, un voire deux mois de calcul intensif sur

LES NOMBRES DE MERSENNE

Marin Mersenne (1588-1648), ou *Marinus Mersenius*, appartenait à l'ordre religieux des Minimes. Érudit, philosophe et mathématicien, il a défini les nombres qui portent son nom. Ils sont de la forme $2^p - 1$. Certains parmi eux sont des nombres premiers. Pour ce faire, p oit lui-même être un nombre premier, cette condition étant nécessaire, mais pas suffisante. Les premiers nombres de Mersenne premiers sont 3 (2^2-1), 7 (2^3-1), 31 (2^5-1), 127 (2^7-1)... Mersenne a calculé (avec quelques erreurs) de tels nombres premiers jusqu'à l'exposant 257. Depuis, c'est la course au plus grand nombre de Mersenne premier, le dernier en date étant pour p = 82 589 933. Avec ses 24 862 048 chiffres, le nombre obtenu est aussi le plus grand nombre premier connu.

Marin Mersenne, un religieux à la culture encyclopédique.

un ordinateur puissant sont nécessaires. Pour cette raison, le *Gimps* distribue les calculs. On peut faire mieux!

Pour ce faire, une première approche consiste à construire une suite basée sur la représentation en base 10 avec, par exemple, $a_{n+1}=10a_n$, et $a_0=7{,}3327334517988679$. On obtient 7, 73, 733, 7333, 73327, 733273... une suite certes de nombres premiers, mais qui s'arrête vite, faute de termes de cette forme qui soient plus grands. C'est l'une des quelques suites connues et la plus étendue. Une autre base bien supérieure à 10, mais de taille fixe, sera forcément prise en défaut, notamment à cause de l'écart entre les nombres premiers qui croît rapidement.

Avec une fonction qui croît plus rapidement, comme n^n on obtient de meilleurs résultats, par exemple avec c=0,265588372943143390897129 45366546... et $a_n = \lfloor cn^n \rfloor$. Elle s'arrête au bout de 19 termes, ici de a_3 à a_{22}. C'est la meilleure qui a été trouvée. Les premiers nombres premiers a_n sont: 7, 67, 829, 12391, 218723, 4455833, 102894377, 2655883729... Et le dernier: 155172317999186449760617 2809.

Encore une fois, et pour les mêmes raisons, le procédé cesse de fonctionner au bout d'un moment. La méthode (*voir l'encadré page suivante*) est fondée sur un programme personnel.

Dans la seconde approche, on considère des formules du type de Mills, celle de Wright étant écartée, car elle croît trop vite. Le problème devient alors de trouver une fonction qui croit suffisamment lentement pour produire une suite de premiers de longueur arbitraire.

Prenons la suite $a_{n+1} = a_n^2 - a_n + 1$, dite de Sylvester (A000058 dans le catalogue OEIS, l'encyclopédie en ligne des suites de nombres entiers). Cette suite commence ainsi, avec a_0=2: a_n = 2, 3, 7, 43, 1807, 3263443, 10650056950807... Tous ne sont pas des nombres premiers ($1807=13\times139$), mais étonnamment, la somme des inverses de ces termes 1/2+1/3 + 1/7+1/43+ 1/1807+1/3263443... est égal à 1. On peut ensuite se demander si l'on peut trouver un a_0 non plus entier, mais réel, qui produise des nombres premiers. Il suffirait d'utiliser la fonction «partie entière» $\lfloor x \rfloor$. La réponse est oui.

Avec a_0=1,6181418093242092, a_n=2, 3, 7, 43, 1811, 3277913, 10744710357637... La croissance est bien inférieure à celle de la formule de Mills et *a fortiori* à celle de Wright. Chaque terme a environ deux fois la taille du précédent, ce qui conduit tout de même à $a_{14} = 9{,}838... \times 10^{1667}$.

Peut-on choisir l'exposant dans la formule précédente de sorte que la croissance soit encore plus lente? Oui, grâce au recuit simulé, on trouve assez rapidement ceci: si a_0=43,80468771580293481... et en utilisant l'arrondi de x noté $\{x\}$, on obtient $S_n=\{a_n\}$ et $a_{n+1}=a_n^{5/4}$. C'est maintenant la suite A323176 du catalogue OEIS: S_n=113, 367, 1607, 10177, 102217...

Cela semble fonctionner! Faisons mieux avec un exposant plus petit et un a_0 choisi soigneusement. Par exemple, si $a_{n+1}= a_n^{11/10}$ et a_0=100000000000000000000000000000049,3 1221074776345... on obtient la suite ci-dessous:

100 000 000 000 000 000 000 000 000 000 049
158 489 319 246 111 348 520 210 137 339 236 753
524 807 460 249 772 597 364 312 157 022 725 894 401
3 908 408 957 924 020 300 919 472 370 957 356 345 933 709
70 990 461 585 528 724 931 289 825 118 059 422 005 340 095 813
3 438 111 840 350 699 188 044 461 057 631 015 443 312 900 908 952 333
48 972 469 000 420 009 426 555 707 142 502 303 667 155 036 417 8496 540 501... >

BIBLIOGRAPHIE

D. FRIDMAN *ET AL.*, A prime-representing constant, *The American Mathematical Monthly*, vol. 126, pp. 70-73, 2019.

Le plus grand nombre premier connu: http://bit.ly/82589933

Le site de Simon Plouffe: http://plouffe.fr

L'OEIS: https://oeis.org/

2
3
5
11
37
223
3 331
192 271
84 308 429
774 116 799 347
681 098 209 317 971 743
562 101 323 304 225 290 104 514 179
13 326 678 220 145 859 782 825 116 625 722 145 759 009
1 538 448 162 271 607 869 601 834 587 431 948 506 238 982 765 193 425 993 274 489

Avec un exposant égal à 3/2 et a_0=2,038239154782... on obtient la suite de nombres premiers ci-dessus.

C'est désormais la suite A323611. Un autre exemple livre les petits nombres premiers. Avec a_0=3,34683553593243081... et un exposant égal à 1,251295195638... la suite (A323065) est: 3, 5, 7, 11, 19, 41, 103, 331, 1423, 8819, 86477, 1504949...

En choisissant a_0 assez grand, on peut utiliser un exposant très petit, comme 101/100. Si a_0=10^{500}+961,4993763378507... on obtient une suite de 100 nombres premiers, le dernier n'ayant que 1340 chiffres. Elle bat ainsi les records de 2010 (58 nombres premiers avec un polynôme et 26 avec une progression arithmétique). Notons néanmoins que lorsque leur taille dépasse 20 chiffres, les nombres obtenus que sont que des premiers probables. Si a_0 est bien choisi, on conjecture que l'exposant peut être aussi près de 1 qu'on le souhaite (pour limiter la croissance).

OBTENIR TOUS LES NOMBRES PREMIERS ?

Avec des formules de ce type, peut-on obtenir tous les nombres premiers? Pour y parvenir, on pourrait par exemple partir d'un nombre premier arbitraire et descendre jusqu'à 2. C'est possible avec un procédé inverse en utilisant 1/α, α étant l'exposant. Ainsi, en partant du nombre premier 10^{100}+267 et avec α =0,38562256415290... on obtient 742123524365563, 542489, 163, 7, 2.

On retrouve la suite inverse en partant à 2 avec a_0=2,1322219996628413452... et l'exposant 1/α=2,5932092490404286167308... Le principe fonctionne dans les deux sens!

Tous ces calculs décrits sont empiriques. En pratique, on arrive à générer un nombre arbitraire de nombres premiers avec une croissance minimale de la suite. Les formules sont bien plus économes que celles Mills et Wright. À partir d'un nombre premier donné, on peut descendre jusqu'à 2 et à partir de 2 on peut obtenir une famille de suites infinies de nombres premiers.

Les records sont faits pour être battus, et avec un matériel informatique adéquat, et un certain temps de calcul, la suite de 100 nombres premiers peut être étendue jusqu'à 1000000 de chiffres. Mieux, lorsque l'exposant est 3/2, on conjecture que tous les nombres premiers peuvent être générés. Reste à le démontrer... ■

UN PROGRAMME MAISON

L'algorithme mis au point procède en trois étapes. D'abord, on choisit la valeur de départ a_0 et l'exposant α, préférablement une fraction simple. Puis on lance un algorithme qui associe la technique de Monte-Carlo (fondée sur des processus aléatoires) et le principe du recuit simulé. Ce principe est inspiré de la métallurgie où l'on alterne les cycles de refroidissement lent et de réchauffage (recuit) afin de minimiser l'énergie d'un matériau. Cette technique évite que l'écart entre chaque nombre premier ne croisse trop vite. Une fois quatre ou cinq valeurs trouvées, on passe à l'étape 3. On utilise une formule qui permet d'aller soit vers l'avant soit vers l'arrière. Vers l'avant, on cherche le plus petit nombre premier après $\{a_p^{\alpha}\}$. C'est assez facile en quelques minutes, même s'il a des milliers de chiffres, grâce à des logiciels, comme Maple ou PFGW. On rebrousse chemin pour vérifier que la formule fonctionne. Pour ce faire, on doit résoudre pour x avec x^{α}- S_{n+1}. Ici S_{n+1} est le prochain nombre premier candidat. C'est ici qu'un α rationnel facilite le calcul.