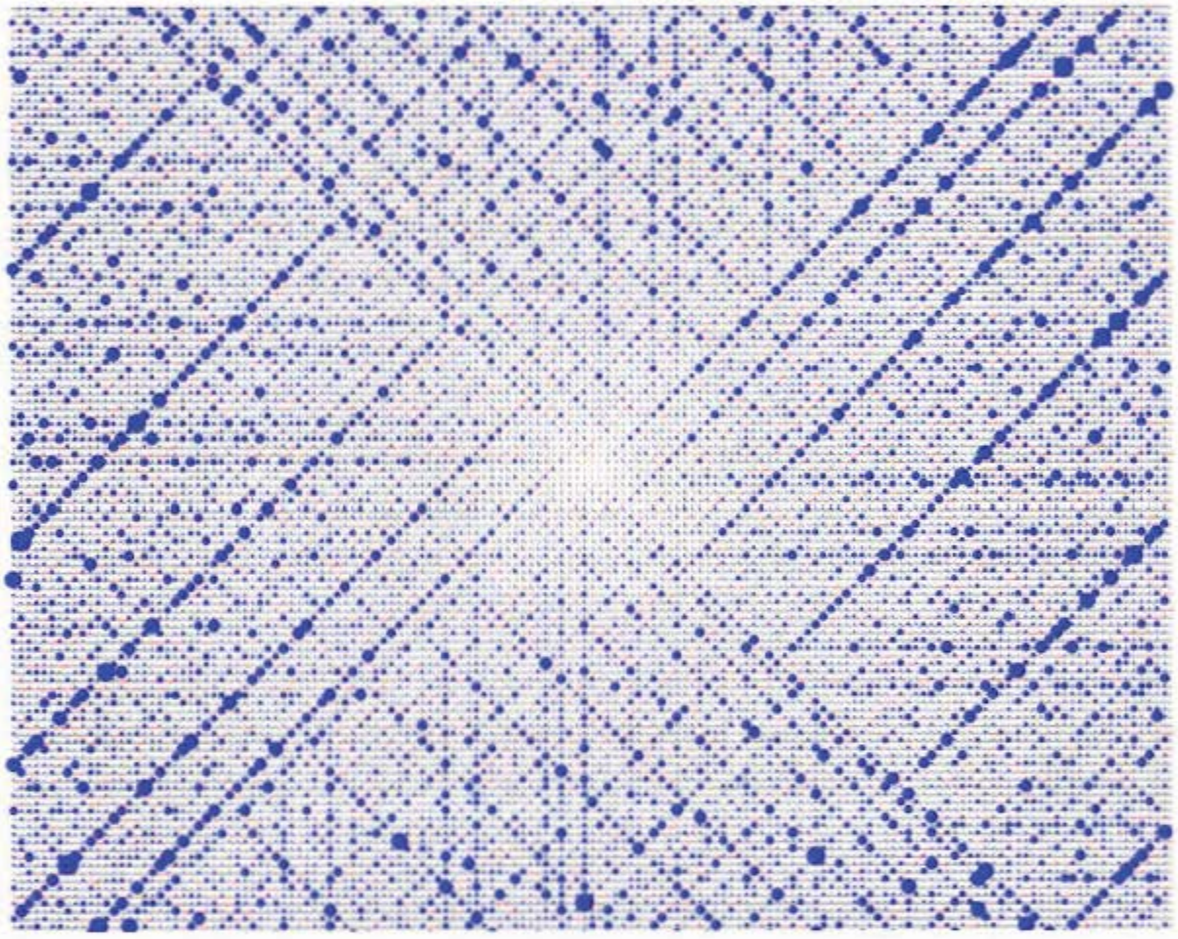
QUÉBEC SCIENCE
Magazine fondé en 1962



SCIENCES

En quête d'une formule pour les nombres premiers

Y a-t-il une formule qui donne tous les nombres premiers? Ou du moins uniquement des nombres premiers? La réponse courte est : ni oui ni non.

MARINE CORNIOU

28-05-2020

Y a-t-il une formule qui donne tous les nombres premiers? Ou du moins uniquement des nombres premiers? La réponse courte est ni oui ni non.

C'est une question vieille de plus de deux millénaires : comment savoir quel nombre premier suit un nombre premier pris au hasard? Par exemple, si l'on regarde la série de ces nombres divisibles uniquement par 1 et par eux-mêmes, on obtient ceci (la liste n'est pas exhaustive bien sûr) : 2, 3, 5, 7, 11, 13, 17, 19... 193, 197, 199... 827... 2 347. Quel est le prochain?

«Tous les grands mathématiciens se sont penchés sur le problème : on peut calculer combien il y a de nombres premiers avant 1 000 ou avant 10 000, mais personne n'a de formule pour trouver directement le $n^{ième}$ nombre premier», résume Simon Plouffe, mathématicien d'origine québécoise et

LES PLUS POPULAIRES

SCIENCES
Ce chant d'oiseau devenu viral au Canada
ANNIE LABRECQUE 07/07/2020

SCIENCES
Les nombres et leurs secrets
QUÉBEC SCIENCE 09/07/2020

professeur au Département d'informatique de l'Institut universitaire de technologie de Nantes.

En fait, pour constituer la liste des nombres premiers, on utilise une technique mise au point il y a plus de 2 000 ans par le savant grec Ératosthène. Elle consiste, à partir de la liste des nombres entiers, à rayer successivement tous les multiples de 2, puis les multiples de 3 (à part 2 et 3 eux-mêmes), et ainsi de suite jusqu'à ce qu'il ne reste que les nombres premiers, indivisibles. Étant donné qu'il y a une infinité de nombres premiers, il y a de quoi faire.

«Avec les ordinateurs, qui font des milliards d'opérations par seconde, la vitesse est faramineuse, mais, à partir d'un certain seuil, le disque sature. On arrive à calculer les nombres premiers jusqu'au 10^{24} ième environ. Après, ça bloque pour des questions de stockage», détaille Simon Plouffe.

Difficile de croire que personne n'a trouvé mieux que cette bonne vieille méthode d'Ératosthène, efficace mais laborieuse.

Essais et erreurs

Ce n'est pourtant pas faute d'avoir essayé. Au 17^{e} siècle, le mathématicien Pierre de Fermat décréta que tous les nombres s'écrivant $2^{2^n} + 1$ étaient premiers. C'est vrai pour $n = 1$ (on obtient 5) et vrai jusqu'à $n = 4$. Mais à partir de $n = 5$, c'est faux tout le temps, du moins pour les innombrables exemples qui ont été testés par ordinateur. Il faut dire que les calculs deviennent vite fastidieux... Pour $n = 5$, on trouve 4 294 967 297, qui s'avère divisible par 641.

Quant à la formule du Suisse Leonhard Euler ($n^2 + n + 41$, proposée en 1772), elle délivre 40 nombres premiers d'affilée pour toutes les valeurs de n entre 0 et 39. Hélas, pour $n = 40$, on trouve 1 681, qui n'est pas premier.

Marin Mersenne, à peu près à la même époque, avait proposé que $2^n - 1$ serait premier si n était lui-même un nombre premier. Ce n'est pas tout le temps vrai, mais ce l'est souvent. C'est d'ailleurs grâce à sa formule qu'on bat régulièrement le record du plus grand nombre premier «de Mersenne» au moyen d'ordinateurs mis en réseau, au sein du projet GIMPS, qui effectuent des calculs avec des nombres vertigineux. En décembre 2018, on a trouvé le 51^{e}, le plus grand connu aujourd'hui : $2^{82\,589\,933} - 1$, un nombre à plus de 24 millions de chiffres (il faudrait un livre de 9 000 pages pour l'écrire).

«En fait, on a un théorème qui dit qu'il n'y a pas de formule facile, tranche Andrew Granville, spécialiste de la théorie des nombres à l'Université de Montréal. C'est impossible d'avoir un polynôme qui donne juste des nombres premiers.» (Un polynôme est une expression formée uniquement de produits et de sommes de constantes et d'inconnues habituellement notées x, y, z...)

EDITO

COVID-19: les scientifiques deviendront-ils des boucs émissaires?

MARIE LAMBERT-CHAN 09/07/2020

Des formules beaucoup plus tirées par les cheveux, et assez peu pratiques, ont été suggérées au 20^{e} siècle, notamment celle de Matiyasevich. «C'est une expression à 26 variables dans laquelle on met toutes les valeurs qu'on veut et, si le nombre est positif, il est premier. Avec toutes les possibilités à chaque étape, si l'on programme la formule dans une machine, elle fait *flop!* Elle en sort un ou deux en une heure et ça s'arrête là. C'est théoriquement résolu, mais à l'époque, on était loin de penser aux aspects informatiques», s'amuse Simon Plouffe.

L'informatique à la rescousse

L'intérêt d'une telle formule est en effet limité si l'on ne peut pas la programmer pour l'appliquer. Et avec la plupart des formules récentes, les nombres augmentent très vite et deviennent ingérables pour les ordinateurs. «C'est un problème de puissance de calcul plus que de théorie», affirme le spécialiste des suites de nombres.

Il propose donc de prendre le problème à l'envers. «Tout le monde s'intéresse à la théorie; moi non. Empiriquement, on peut trouver mieux que toutes les formules actuelles.» Par «empiriquement», il entend, en gros, partir d'une grande quantité de nombres premiers et trouver un lien entre eux.

En 2019, Simon Plouffe a battu un record en générant une formule «simple» capable de donner 50 nombres premiers, puis 100. Un record! «Depuis, j'en ai produit une autre qui délivre une infinité de nombres premiers, mais qui grossissent moins vite. J'ai un algorithme qui utilise le principe du "recuit" : la machine sort des nombres au hasard, je lui demande de ne garder que ceux qui sont premiers et de se concentrer sur ces cas-là», explique-t-il.

En juin 2020, le chercheur a même poussé sa formule (sous la forme d'une suite $\{c^k\}$, c étant une constante à rallonge) pour générer pas moins de 633 nombres premiers d'affilée. « Cette formule est la plus simple qui soit et pourtant, c'est la première fois qu'on peut générer des nombres premiers comme ça, si facilement », indique-t-il.

Cette forme de mathématiques expérimentales ne convainc pas les théoriciens, car on ne peut en tirer aucune preuve générale. Simon Plouffe n'en a que faire et compte bien poursuivre ses efforts, avec ses ordinateurs «de base» qui calculent en continu. «En raffinant encore la méthode, je pense que je peux produire une formule qui donnerait le $n^{ième}$ nombre premier directement. C'est mon rêve. Il faut juste y penser numériquement.»

On le croit sur parole : ce passionné de nombres, qui pouvait réciter de mémoire plus de 4 000 décimales de pi dans sa jeunesse, est à l'origine d'une formule qui permet de calculer le $n^{ième}$ chiffre après la virgule du nombre π sans avoir à en calculer les précédents. Nommée formule BBP (ou formule de Bailey-Borwein-Plouffe, du nom des trois auteurs), elle a été élaborée en 1995. «Il n'y a

pas de problème impossible pour un cœur vaillant, affirme ce mathématicien coloré. Il y a toujours moyen de trouver une astuce de calcul.»