ÉCLATS DE SCIENCES

Les nombres premiers révèlent certains de leurs mystères

Mathématiciens et amateurs s'échinent depuis des siècles à mieux comprendre ces étranges nombres qualifiés de premiers. Récemment, leurs efforts ont été récompensés par de nouvelles découvertes, qui pourraient avoir des applications dans le domaine de la cryptographie.

Charlotte Mauger - 7 décembre 2024 à 10h50

2, 3, 5, 7, 11, 13, 17, 19… cette liste n'a rien de banal : c'est celle des nombres premiers. Le plus grand – à ce jour – vient d'être trouvé par un passionné. Il s'agit d'un monstre de 41 millions de chiffres qui se calcule en multipliant plus de 100 millions de fois le chiffre 2 par lui-même, moins 1 : $2^{136\,279\,841} - 1$. Mais ce n'est pas seulement une curiosité mathématique. Car lui et l'ensemble des nombres premiers fascinent les scientifiques, tant leur apparition semble aléatoire. Ils jouent désormais un rôle crucial dans la cryptographie, en sécurisant nos transactions bancaires, par exemple.

Mais que sont ces nombres, qualifiés de « premiers » ? Ils peuvent être définis très simplement : ce sont des nombres qui ont la particularité de ne pouvoir être divisés que par eux-mêmes et par 1. Comme 13, dont la division par n'importe quel autre nombre donnerait un résultat non entier, c'est-à-dire avec des chiffres après la virgule.

Mais surtout, ce sont les stars des mathématiques, et en particulier de la théorie des nombres, cette branche qui étudie les entiers. *« On peut les voir comme les briques élémentaires des nombres »*, explique Cathy Swaenepoel, chercheuse à l'université Paris-Cité. Des briques élémentaires, avec lesquelles on peut reconstruire tous les nombres. Chacun s'écrit comme un produit de premiers, comme 126 qui est la multiplication 2 × 3 × 3 × 7.

Une définition simple, un rôle clé en mathématiques mais surtout de grandes interrogations. Si l'on regarde attentivement la liste, on voit qu'ils n'apparaissent pas de façon régulière. Par exemple, 139, 149 et 151 sont trois nombres premiers successifs.

« On sait même qu'il y a des intervalles arbitrairement grands dans lesquels il n'y a aucun nombre premier », précise Cécile Dartyge, mathématicienne à l'Institut Élie Cartan (université de Lorraine). Ce qui veut dire qu'à un moment donné dans la liste, il y aura un trou de 1 000 entiers sans aucun premier, un autre de 7 millions, un également de 18 milliards, sans qu'on sache forcément où. *« C'est donc vraiment mystérieux, on ne sait pas comment ils sont répartis »*, souligne la chercheuse.

Un nombre de 41 millions de chiffres

Comment y voir plus clair ? Une première idée serait de trouver un à un chaque nombre premier, afin de mieux comprendre où ils se cachent. Disons-le tout de suite, c'est une entreprise vaine, car il y a une infinité de nombres premiers. Néanmoins, des passionné·es se lancent dans cette aventure durant leur temps libre. C'est ainsi qu'est arrivée la dernière réussite en date, la trouvaille du nombre $2^{136\,279\,841} - 1$. Un nombre de plus de 41 millions de chiffres, si gigantesque qu'il faudrait 10 423 pages A4 en Arial 11 pour l'écrire dans sa totalité. Il a été découvert par Luke Durant, un ancien employé de l'entreprise de processeurs graphiques Nvidia, dans le cadre du projet GIMPS, pour Grande Recherche des premiers de Mersenne sur Internet.

Cela ne veut pas dire pour autant qu'on connaît tous les nombres premiers entre 2 et $2^{136\,279\,841}$ -1. Il est trop difficile de tester tous les nombres un à un pour voir s'ils sont premiers, même pour un supercalculateur. Alors, pour les trouver, il est plus commun de ne regarder que des nombres d'un type particulier, comme ceux dits de Mersenne. *« Ces nombres s'écrivent sous la forme $2^p - 1$, où "p" est un autre nombre premier. Dans un sens, cela les rend beaucoup plus simples que les autres*, détaille l'heureux découvreur à Mediapart. *En effet, les mathématiciens ont trouvé des manières de tester si ces nombres sont premiers beaucoup plus rapidement que*

pour n'importe quel autre nombre ! »

« *Grâce à ce type de projet, on peut mieux comprendre les nombres premiers de Mersenne car on en connaît très peu, seulement 52* », explique Reginald McLean, un développeur qui investit son temps libre sur le site PrimePages pour lister les découvertes des nombres premiers. Surtout que les mathématicien·nes supposent qu'il existe en fait une infinité de nombres premiers de Mersenne…

En quête d'une formule

Cette méthode manuelle est utile mais ne peut pas conduire à des résultats généraux de mathématiques. Car aussi grands soient-ils, ces nombres sont négligeables face à l'infinité de nombres premiers. Alors, la meilleure manière pour les comprendre serait de trouver une formule, pas trop complexe, qui les calcule dans l'ordre. « *Ce serait génial, mais on n'a pas de telle formule !* », prévient Cathy Swaenepoel.

Les nombres premiers ne se laissent pas facilement capturer. Pour grappiller des connaissances, les spécialistes de l'arithmétique doivent se contenter de questions autour de leur répartition : combien y a-t-il de nombres premiers plus petits que 10 000 ou 10 milliards ? Combien sont séparés d'un seul nombre ? Combien s'écrivent comme la somme de deux carrés ?

« *Et on a fait beaucoup de progrès grâce à ce genre de questions* », souligne Cécile Dartyge. L'un des bonds en avant fut la démonstration du théorème des nombres premiers, en 1896, par Jacques Hadamard et Charles-Jean de La Vallée Poussin. Ce résultat permet d'estimer combien de premiers se trouvent entre 2 et un nombre x aussi grand qu'on veut. Avec cette formule magique, on détermine par exemple qu'il y a, à peu près, 145 premiers entre 2 et 1 000.

Mais on sait aussi que cette formule n'est pas tout à fait exacte : il y a en réalité 168 premiers plus petits que 1 000, et non 145. Des travaux tentent d'ailleurs d'estimer la marge d'erreur entre la valeur obtenue par la formule et la quantité réelle de nombre premiers.

C'est dans ce contexte que l'hypothèse de Riemann entre en scène. Il s'agit d'une conjecture, un résultat que les mathématicien·nes supposent vrai mais qu'ils voudraient prouver pour en être sûrs. Et surtout, c'est l'une des questions majeures des mathématiques, puisqu'elle fait partie des sept très difficiles « problèmes du millénaire », qui vaudront 1 million de dollars à celles et ceux qui réussiront à les résoudre. Si l'hypothèse de Riemann est vraie, alors cette marge d'erreur serait faible.

Des progrès récents

Reste que pour l'heure, l'hypothèse de Riemann n'a toujours pas été prouvée. Un pas vient toutefois d'être franchi dans cette voie. Dans un article non relu par les pairs, les mathématiciens Larry Guth, du Massachusetts Institute of Technology (MIT), et James Maynard, de l'université d'Oxford, se sont attaqués à ce problème du millénaire et l'ont fait progresser. « *Une conséquence de leurs travaux est une amélioration de l'estimation des premiers dans de petits intervalles* », explique Cécile Dartyge.

Mais pour comprendre les nombres premiers, les mathématicien·nes ne font pas que les compter. D'autres s'intéressent à ceux qui ont une forme particulière. « *Au lieu de regarder tous les entiers, on ne regarde que ceux qui ont une certaine forme et on étudie les nombres premiers là-dedans. Il y a une grande motivation autour de ces problèmes* », appuie Cathy Swaenepoel.

Par exemple, dans un autre récent article (non relu par les pairs), Ben Green et Mehtaab Sawhney, respectivement mathématiciens à Oxford et Columbia, ont regardé les nombres premiers qui s'écrivent presque comme la somme de deux carrés de nombres premiers. Plus précisément, qui s'écrivent comme $p^2 + n \times q^2$, avec p et q premiers et n multiple de 6 ou multiple de 6 auquel on ajoute 4. C'est le cas du premier 61, qui est égal à $5^2 + 4 \times 3^2$. Or, ils ont trouvé qu'un nombre infini de premiers s'écrivent sous cette forme.

Cela peut sembler anecdotique, mais il n'en est rien : il y a très peu d'entiers qui se décomposent ainsi, et malgré cela, il y a quand même une infinité de nombre premiers. Comme s'ils se glissaient un peu partout.

Des transactions sécurisées

Tous ces travaux ressembleraient à une entreprise de spécialistes œuvrant dans un cercle fermé si nous n'étions pas au contact des nombres premiers tous les jours. En effet, ils interviennent dès lors qu'on échange des informations en toute sécurité sur Internet (notamment lors d'une transaction bancaire).

« *Depuis les années 1970, les nombres premiers ont permis une révolution dans le monde de la cryptographie en permettant des chiffrements asymétriques* », explique Anne-Gwénaëlle de Roton, mathématicienne à l'Institut Élie Cartan. Un chiffrement symétrique, c'est comme donner la clé et le cadenas à la personne qui nous envoie des informations confidentielles ; l'asymétrique, c'est donner un cadenas ouvert mais garder la clé bien précieusement. Ainsi, l'échange est sûr sans avoir besoin d'envoyer la clé.

Que viennent faire ici les nombres premiers ? Tout est basé sur un constat simple : « *Si on multiplie deux grands nombres premiers, on trouve le résultat facilement. Par contre à partir du résultat, il est très difficile de retrouver les deux premiers de départ* », affirme la chercheuse. Pour preuve, il est très difficile de se rendre compte à la main que 34 833 059 est le produit des premiers 4 421 et 7 879. Même les ordinateurs sont mauvais pour réussir cette devinette quand les nombres de départ sont très grands.

Ainsi, si vous annoncez publiquement le produit de deux très grands nombres premiers, il y a un très faible risque que des personnes malintentionnées retrouvent ces deux nombres (même s'ils sont spécialistes des nombres premiers !). Ce produit, c'est la clé de chiffrement qui rend secret votre message ou votre code bancaire. Pour la déchiffrer, il faut retrouver les deux nombres premiers derrière cette clé. Ce qui est impossible. « *Ainsi, l'étude des nombres premiers permet aussi de comprendre à quel point ces systèmes sont sûrs !* », ajoute Cathy Swaenepoel.

Avec la puissance croissante des ordinateurs, il est nécessaire d'utiliser des nombres premiers de plus en plus grands pour que les protocoles restent sûrs (autour de 1 200 chiffres). Alors, qui sait, peut-être que l'énormissime $2^{136\,279\,841} - 1$ sera utile pour sécuriser nos transactions dans quelques années !

Charlotte Mauger