Le théorème de Green-Tao et autres secrets des nombres premiers

Michel Waldschmidt, *professeur émérite à l'Université Pierre et Marie Curie*

Bien que les mathématiciens s'y intéressent depuis l'Antiquité, les nombres premiers continuent de fasciner. En les additionnant ou en les soustrayant entre eux, on trouve une mine de problèmes dont certains sont longtemps demeurés ouverts ou restent encore irrésolus.

Obtenir tous les nombres entiers positifs en utilisant les seuls symboles + et 1 est facile : il suffit d'écrire chaque entier $n > 0$ sous la forme 1 + 1 + … + 1 avec n fois le symbole 1 et (n-1) fois le symbole +.

Remplaçons l'addition par la multiplication et le symbole + par le symbole x (ou •). Pour écrire tous les nombres entiers positifs comme des produits, on a donc besoin de *briques* élémentaires qui jouent le rôle tenu par 1 pour l'addition. Ces briques sont les *nombres premiers*, ceux qui ne peuvent pas s'écrire comme produits de nombres entiers plus petits. Chaque entier supérieur ou égal à 2 est produit, de manière unique (à permutations près), de nombres premiers : c'est ce qu'on appelle le *théorème fondamental de l'arithmétique*. Par exemple 4200 = 2 x 2 x 2 x 3 x 5 x 5 x 7.

Des nombres aussi grands que l'on veut

La liste des nombres premiers commence par 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37…

On trouve le début de cette liste sur la toile, dans l'encyclopédie des suites de nombres entiers, qui est une mine d'informations pour ce genre de questions. Les nombres supérieurs à 1 qui ne sont pas premiers sont appelés nombres *composés*. Leur liste commence par 4, 6, 8, 9, 10, 12, 14, 15, 16…

Cette deuxième liste comporte entre autres tous les nombres pairs à partir de 4. Il est donc facile d'écrire un nombre composé aussi grand que l'on veut. En revanche, écrire (par exemple sous forme décimale) un nombre premier aussi grand que l'on voudrait est une opération que l'on ne sait pas réaliser.

Le plus grand nombre premier explicitement connu (depuis le 2 mai 2013) est $2^{57\,885\,161} - 1$ qui a 17 425 170 chiffres décimaux. Si on écrivait tous ces chiffres avec disons deux chiffres par centimètre, l'écriture de ce nombre s'étendrait sur plus de 87 kilomètres !

Pourtant on sait, depuis Euclide, que la liste des nombres premiers ne s'arrête jamais : *il existe une infinité de nombres premiers*. Les nombres premiers sont donc un exemple de suite dont on sait qu'elle est infinie, mais dont on ne sait pas expliciter des éléments aussi grands que l'on voudrait.

Des propriétés additives étonnantes

Les nombres premiers ont été introduits en arithmétique pour la multiplication, comme nous venons de le voir. Étudier leurs propriétés additives peut sembler une idée bizarre. Elle mène cependant à des problèmes profonds, dont l'étude a conduit à des théories très élaborées d'une grande richesse, nécessitant l'utilisation d'outils mathématiques sophistiqués. Le plus fascinant dans cette théorie est qu'elle continue à se développer. Elle a permis de résoudre un grand nombre de questions qui sont restées ouvertes fort longtemps, mais elle n'est pas encore suffisamment puissante pour répondre à certaines questions qui sont pourtant faciles à formuler.

Additionnons deux nombres premiers ; on obtient les valeurs suivantes :

p	2,	3,	5,	7,	11,	13,	17,	19,	23,	29,	31,	37...
$p + 2$	4,	5,	7,	9,	13,	15,	19,	21,	25,	31,	33,	39...
$p + 3$	5,	6,	8,	10,	14,	16,	20,	22,	26,	32,	34,	40...
$p + 5$	7,	8,	10,	12,	16,	18,	22,	24,	28,	34,	36,	42...
$p + 7$	9,	10,	12,	14,	18,	20,	24,	26,	30,	36,	38,	44...
$p + 11$	13,	14,	16,	18,	22,	24,	28,	30,	34,	40,	42,	48...
...	...											

Les seuls nombres impairs que l'on puisse trouver dans ce tableau figurent sur la première ligne (celle qui donne les $p + 2$) et sur la première colonne (celle qui donne les $2 + p$, puisque le tableau est symétrique). En effet, la somme de deux nombres impairs est forcément un nombre pair. Comme 2 est le seul nombre premier pair, les seules sommes impaires de deux nombres premiers sont celles qui consistent à ajouter 2 à un nombre premier impair ; toutes les autres sommes sont des nombres pairs.

Ce qui est remarquable est qu'il semble qu'on obtienne avec ce tableau tous les nombres pairs à partir de 4. Beaucoup de nombres pairs sont obtenus de plusieurs façons différentes, par exemple,

10 = 5 + 5 = 7 + 3 ; 14 = 7 + 7 = 3 + 11…

Que tous les nombres pairs supérieurs ou égaux à 4 puissent s'écrire comme somme de deux nombres premiers est un problème ouvert.

Que tous les nombres pairs supérieurs ou égaux à 4 puissent s'écrire comme somme de deux nombres premiers est appelé problème binaire de Goldbach ; il a été proposé par Euler en réponse à une lettre de Goldbach datant de 1742, dans laquelle Goldbach suggérait que tout nombre entier supérieur ou égal à 7 était somme de trois nombres premiers. Ce dernier résultat, moins fort que le problème binaire de Goldbach, a été annoncé par Harald Helfgott en mai 2013. Mais le problème binaire de Goldbach est toujours ouvert et c'est la source de nombreuses recherches depuis bientôt trois siècles. C'est un problème difficile, qui a donné naissance à des théories élaborées ayant d'autres applications. On peut citer par exemple la théorie additive des nombres, qui étudie les sommes de nombres entiers appartenant à un ensemble donné (ici les nombres premiers).

La différence entre deux nombres premiers : une source de questions passionnantes

Une autre façon de marier les nombres premiers avec l'addition consiste à étudier la différence entre deux nombres premiers consécutifs.

La liste des nombres premiers est $(p_1, p_2, p_3 \dots) = (2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37 \dots)$ et la liste $(p_n - p_{n-1})$ des différences entre deux nombres premiers consécutifs commence par 1, 2, 2, 4, 2, 4, 2, 4, 6, 2, 6…

Il est facile de voir qu'à part la première valeur, 1, toutes les autres sont des nombres pairs : cela provient une fois de plus du fait que 2 est le seul nombre premier pair. Y a-t-il une infinité de 2 dans cette liste ? On ne le sait pas encore ; c'est la conjecture des nombres premiers jumeaux, qui s'énonce : *il existe une infinité de nombres premiers p ayant la propriété que $p + 2$ est aussi premier.*

On sait que la suite des différences entre deux nombres consécutifs de la suite des nombres premiers n'est pas bornée : il existe des « trous » aussi grands qu'on veut (l'étude des « trous » dans la suite des nombres premiers remonte à Legendre et Gauss). On sait aussi estimer l'ordre de grandeur moyen de tels trous, grâce au Théorème des Nombres Premiers, démontré en 1896 par Hadamard et de la Vallée Poussin. La légende prétendait que le mathématicien qui démontrerait cette conjecture serait immortel. D'une certaine manière Jacques

Hadamard (1865-1963) et Charles de la Vallée Poussin (1866-1962) laissent leur nom dans l'histoire par leur théorème, mais ils ont aussi réalisé la prédiction de façon aussi complète que possible, puisqu'ils sont décédés presque centenaires.

Récemment, de nouveaux progrès ont été accomplis sur la question des trous entre deux nombres premiers. Le postulat de Bertrand, démontré par Tschebycheff vers 1850, affirme qu'entre un nombre entier et son double, il y a toujours un nombre premier.

Au lieu du coefficient 2 qui intervient dans le double, on peut prendre n'importe quel facteur $c > 1$: pour n suffisamment grand, il y a toujours un nombre premier p entre n et cn. Cela donne déjà une information sur les écarts entre deux éléments consécutifs de la suite des nombres premiers. Le théorème des nombres premiers implique plus précisément que la différence entre le n-ième nombre premier p_n et le suivant p_{n+1} est de l'ordre de grandeur de log p_n, le logarithme népérien de p_n.

En 2013, Yitang Xang a démontré qu'il existe une infinité de couples de nombres premiers dont l'écart est inférieur à 70 millions.

C'est loin de ce que l'on attend, si on pense à la conjecture des nombres premiers jumeaux ci-dessus, selon laquelle la différence entre deux nombres consécutifs de la liste des nombres premiers devrait être 2 une infinité de fois. Mais c'est un progrès considérable par rapport à ce que l'on savait avant.

Progressions arithmétiques

L'étude des différences entre les nombres premiers peut être généralisée d'une autre manière, en étudiant les progressions arithmétiques composées de nombres premiers. Une suite de nombres forme une *progression arithmétique* si la différence entre deux termes consécutifs de la suite est toujours la même : cette valeur est alors la *raison* de la progression.

Par exemple la suite 5, 11, 17, 23, 29 est une progression arithmétique de 5 termes de raison 6.

La suite 7, 37, 67, 97, 127, 157 est une progression arithmétique de 6 termes de raison 30 et la suite 199, 409, 619, 829, 1039, 1249, 1459, 1669, 1879, 2089 est une progression arithmétique de 10 termes de raison 2100. Dans ces exemples, les termes de ces suites sont tous des nombres premiers.

Y a-t-il des progressions arithmétiques aussi longues que l'on veut composées uniquement de nombres premiers ?

La plus longue progression arithmétique explicitement connue composée uniquement de nombres premiers comporte 26 termes, la raison en est le produit de 23 681 770 par 223 092 870 ; c'est la suite 43 142 746 595 714 191 + 23 681 770 · 223 092 870 n pour n prenant les valeurs de 0 à 25. Elle a été trouvée par Benoît Perichon.


Ben Green


Terence Tao

Y a-t-il des progressions arithmétiques aussi longues que l'on veut composées uniquement de nombres premiers ? Pendant longtemps cette question a été ouverte, c'était encore un défi de plus pour les mathématiciens. C'est un travail mené en collaboration par les mathématiciens Ben Green et Terence Tao qui a conduit finalement à la solution en 2004. Leur théorème dit ainsi que oui, il existe des progressions arithmétiques, de longueur aussi grande que l'on veut, composées uniquement de nombres premiers. Leur démonstration n'est pas constructive, c'est-à-dire qu'elle ne dit pas comment construire une telle suite !

Pour aller plus loin

Tenenbaum G., Mendès-France M., (1997). *Les Nombres premiers*; Presses Universitaires de France (PUF), coll. Que Sais-je ?.

Ribenboim P., (2000). *Nombres premiers : mystères et records*; Presses Universitaires de France (PUF), coll. Mathématiques.

Hardy G.H., Wright E.M., (2008). *An Introduction to the Theory of Numbers*; Oxford Science Publications, sixth ed. Oxford : Oxford University Press. Revised by D. R. Heath-Brown and J. H. Silverman, With a foreword by Andrew Wiles.

Sur Internet

http://www.mersenne.org/
http://primes.utm.edu/largest.html
https://oeis.org/

Le blog de Terence Tao :
http://terrytao.wordpress.com/