On sait depuis Euclide qu'il y a un nombre infini de nombres premiers. Leur structure semble aléatoire. On observe des intervalles très grands sans nombres premiers, et on semble aussi observer une infinité de nombres premiers jumeaux comme 9719 et 9721. Pourtant les nombres premiers ont une structure. En comprendre les détails ne cesse de fasciner les mathématiciens, et certains de ces résultats ont été couronnés par une médaille Fields en 2022.

Comprendre la structure

Andrew Granville
Université de Montréal

Dans toutes les sciences on cherche les constituants de base : comprendre leur structure permet de comprendre la structure des composés. En physique, les composants de base sont les particules élémentaires, en chimie, les atomes. Dans la science du vivant, c'est l'ADN. Et en théorie des nombres, ce sont les nombres premiers. Chaque entier naturel différent de 0 et 1 est caractérisé par sa décomposition en facteurs premiers et celle-ci nous en apprend beaucoup sur les propriétés du nombre.

En lisant les *Éléments* d'Euclide, nous savons que les Grecs de l'Antiquité ont compris que tout nombre entier positif a une factorisation unique en puissances de nombres premiers (sans se soucier de l'ordre des facteurs), ce qui les a conduits à commencer à s'interroger sur les propriétés des nombres premiers eux-mêmes. La première question à laquelle ils ont répondu était de savoir s'il y en avait une infinité. Euclide donne une preuve qu'il y en a une infinité dans son livre, et aujourd'hui nous avons littéralement des millions de preuves différentes.

Une fois que l'on sait qu'il y a une infinité de nombres premiers, il est naturel de se demander combien il y en a jusqu'à un nombre donné, par exemple combien de nombres premiers inférieurs à un million, ou un milliard, ou plus encore. Regardons la table de la page suivante. La deuxième colonne $\pi(x)$ donne le nombre de nombres premiers inférieurs ou égaux à x.

On constate que $\pi(x)$ croît rapidement avec x. En effet, le pourcentage, $\pi(x)/x$, des entiers premiers inférieurs ou égaux à x, décroit régulièrement de 16,8 % et 12,3 % dans la première et la deuxième rangée à

$$\dots, 2,014\,\%,\ 1,925\,\%,\ 1,844\,\%,\ 1,768\,\%,\ 1,699\,\%,\ 1,635\,\%,\dots$$

pour les dernières rangées, soit une décroissance lente. Si nous jouons avec cela, nous pouvons découvrir qu'en multipliant le rapport $\pi(x)/x$ pour $x = 10^N$ par N (colonne 3), nous nous rapprochons de la constante 0,442 qui est un peu plus grande que $1/\ln(10) \approx 0{,}434\,294$. En mettant ces observations ensemble, nous devinons à partir de ces données que

$$\pi(x) \text{ est bien approximé par } \frac{x}{\ln x}$$

(comparer colonnes 2 et 4). Une autre manière de le voir est de regarder les rapports

$$\pi(x)\Big/\frac{x}{\ln x}$$

pour les x de notre tableau (colonne 5): ces rapports sont supérieurs à 1, mais semblent converger vers 1 à mesure que x augmente.

Lorsque Gauss était adolescent, à la fin du XVIII^e^ siècle, il y avait relativement peu de données disponibles sur les nombres premiers, mais Gauss, à la main, a déterminé combien de nombres premiers il y avait dans les différents intervalles de longueur 1000 jusqu'à 3 millions.

Bien des années plus tard, il a écrit[1] :

En 1792 ou 1793… j'ai porté mon attention sur la fréquence décroissante des nombres premiers… en comptant les nombres premiers dans des intervalles de longueur 1 000. J'ai vite compris que derrière toutes ces fluctuations, cette fréquence est en moyenne inversement proportionnelle au logarithme…

lorsque t varie de 2 à x. Quand on veut tenir compte de l'effet global d'une quantité qui varie quand t varie, il est naturel de prendre une intégrale. Ceci a suggéré à Gauss l'approximation suivante

$$\int_2^x \frac{dt}{\ln t},$$

que nous désignons par Li(x) (et qui est appelée logarithme intégral). Cette approximation est meilleure. Dans la table (colonne 6) on voit que pour chaque valeur de x, Li(x) est une excellente approximation de $\pi(x)$:

e des nombres premiers

Les mêmes observations qu`à la ligne 3 de la citation peuvent être reformulées ainsi

Environ 1 sur ln t des entiers de l'ordre de t sont premiers.

À première vue, cela confirme notre estimation de $x/\ln x$, mais une telle estimation ne tient pas compte de la façon dont $1/\ln t$ varie

1. *Lettre de K.F. Gauss à Johann Franz Encke, veille de Noël 1849*

en effet, les nombres de la colonne Li(x) – $\pi(x)$ sont moitié moins longs que ceux de la colonne de gauche (dans leur écriture décimale), et sont donc de l'ordre de la racine carrée de x, ce qui laisse supposer que $|\pi(x) - \text{Li}(x)|$ est peut-être toujours inférieur à $\sqrt{x}$, ou quelque chose comme ça.[2]

2. *On a de bonnes raisons de croire que $|\pi(x) - Li(x)| < \sqrt{x}\ln x$ dès que $x \geq 100$.*

$x = 10^N$	$\pi(x)$	$\frac{N\pi(x)}{x}$	$\frac{x}{\ln x}$	$\frac{\pi(x)}{x/\ln x}$	$\text{Li}(x) - \pi(x)$	$\frac{\text{Li}(x) - \pi(x)}{\pi(x)}$
10^3	168	0,504	145	1,59	10	0,059
10^4	1229	0,492	1085	1,32	17	0,0017
10^5	9592	0,480	8586	1,12	38	0,0138
10^6	78498	0,471	72382	1,08	130	0,0135
10^7	664579	0,465	620421	1,07	339	0,0051
10^8	5761455	0,461	5428681	1,06	754	0,0014
10^9	50847534	0,458	48254942	1,05	1701	$0{,}33\times10^{-4}$
10^{10}	455052511	0,455	434294482	1,05	3104	$0{,}68\times10^{-5}$
10^{11}	4118054813	0,453	3948131654	1,04	11588	$0{,}28\times10^{-6}$
10^{12}	37607912018	0,451	36191206825	1,04	38263	$0{,}10\times10^{-7}$
10^{13}	346065536839	0,450	334072678387	1,04	108971	$0{,}31\times10^{-8}$
10^{14}	3204941750802	0,449	3102103442166	1,03	314890	$0{,}98\times10^{-9}$
10^{15}	29844570422669	0,448	28952965460217	1,03	1052619	$0{,}35\times10^{-9}$
10^{16}	279238341033925	0,447	271434051189532	1,03	3214632	$0{,}15\times10^{-9}$
10^{17}	2623557157654233	0,446	2554673422960305	1,03	7956589	$0{,}30\times10^{-10}$
10^{18}	24739954287740860	0,445	24127471216847324	1,03	21949555	$0{,}89\times10^{-11}$
10^{19}	234057667276344607	0,445	228576043106974646	1,02	99877775	$0{,}43\times10^{-11}$
10^{20}	2220819602560918840	0,444	2171472409516259138	1,02	222744644	$0{,}10\times10^{-11}$
10^{21}	21127269486018731928	0,444	20680689614440563221	1,02	597394254	$0{,}28\times10^{-12}$
10^{22}	201467286689315906290	0,443	197406582683296285296	1,02	1932355208	$0{,}96\times10^{-13}$
10^{23}	1925320391606803968923	0,443	1888236877840225337614	1,02	7250186216	$0{,}38\times10^{-13}$
10^{24}	18435599767349200867866	0,442	18095603412635492818797	1,02	17146907278	$0{,}93\times10^{-14}$
10^{25}	176846309399143769411680	0,442	173717792761300731060452	1,02	55160980939	$0{,}31\times10^{-14}$
10^{26}	1699246750872437141327603	0,442	1670363391935583952504342	1,02	155891678121	$0{,}92\times10^{-15}$
10^{27}	16352460426841680446427399	0,442	16084980811231549172264034	1,02	508666658006	$0{,}31\times10^{-15}$

Une autre observation de notre tableau est que la sixième colonne semble toujours être positive. Ceci semble suggérer qu'il y a peut-être un autre terme que nous pourrions introduire dans notre approximation de $\pi(x)$ qui rendrait le terme d'erreur encore plus petit. Dans ce cas, les données de la table sont trompeuses et ce ne sera pas toujours le cas que $\mathrm{Li}(x) > \pi(x)$. Nous savons maintenant que $\mathrm{Li}(x)$ et $\pi(x)$ se coupent une infinité de fois: il existe des nombres x, arbitrairement grands, tels que $\mathrm{Li}(x)$ est plus petit que $\pi(x)$ et aussi des nombres y, arbitrairement grands, tels que $\mathrm{Li}(y)$ est plus grand que $\pi(y)$. Nous ne savons pas vraiment quand la première intersection se produit. Mais, nous savons avec certitude que la première intersection se produit avant $1{,}4 \times 10^{316}$ et nous soupçonnons qu'elle se produit à peu près à ce moment-là. Cependant, les nombres en jeu sont tellement grands qu'un calcul exact est impossible et qu'il est difficile de confirmer ce soupçon.

Des patrons dans les nombres premiers ?

Y a-t-il un patron quand on regarde la suite des nombres premiers

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, \ldots ?$$

Il n'y a rien qui saute aux yeux immédiatement. Alors, faisons quelques observations simples. Pour commencer, tous les nombres premiers, sauf le premier, 2, sont impairs. Or, les entiers impairs diffèrent d'au moins 2, de sorte que l'écart entre toute paire de nombres premiers distincts supérieurs ou égaux à 3 est au moins 2. Nous voyons que l'écart 1 entre les nombres premiers ne se produit qu'une seule fois (entre 2 et 3). Alors, qu'en est-il de l'écart 2 ? Ne se produit-il également qu'un nombre fini de fois ? Ou bien existe-t-il une infinité de paires de *nombres premiers jumeaux* ?

En regardant les données, nous trouvons les paires

$$3\&5;\ 5\&7;\ 11\&13;\ 17\&19;\ 41\&43;\ 59\&61;\ 71\&73;\ 101\&103;\ 107\&109;\ \ldots$$

et les calculs à l'ordinateur permettent de poser la conjecture suivante

Conjecture des nombres premiers jumeaux :

Il y a une infinité de paires de nombres premiers jumeaux.

Cette conjecture est encore ouverte. Pourquoi semble-t-elle si difficile à résoudre ? Peut-être est-ce parce que les nombres premiers sont une caractéristique des propriétés multiplicatives, alors qu'une différence de 2 entre deux nombres est une propriété additive ? Alors, comment mélanger les deux ? Souvent en mathématiques quand on ne sait pas répondre à une question on élargit la question. Ici on peut regarder d'autres différences que 2 entre deux nombres premiers consécutifs. On peut par exemple se demander s'il existe une infinité de paires de nombres premiers de la forme p, $p + 4$, ou de la forme p, $p + 6$, ou encore de la forme p, $p + 2k$ pour tout entier pair donné $2k \geq 2$.[3] Ces questions semblant encore hors de portée, les mathématicien.ne.s se sont concentré.e.s sur une approche sur laquelle il.elle.s pouvaient progresser en élargissant encore leurs questions :

3. *Prouvez que 2, 5 est la seule paire de nombres premiers différant de 3 ; que 2 et 7 est la seule paire de nombres premiers différant de 5 ; et qu'il n'existe aucune paire de nombres premiers différant de 7.*

Yitang Zhang

Yitang Zhang, né en 1955, est un mathématicien chinois qui a obtenu son doctorat en 1991. N'ayant pas obtenu de poste universitaire, il a poursuivi ses recherches en parallèle d'une carrière de comptable et d'un emploi dans un restaurant Subway. En 2013, il a donné une réponse positive à la question $\mathbf{Q}_1$. Son résultat spectaculaire de 2013 lui a finalement valu un poste universitaire à partir de 2014. Le film *Counting from Infinity* (Zala Films, 2015) relate sa vie fascinante.

Q$_1$ Existe-il un entier pair $2k$ pour lequel on a une infinité de paires de nombres premiers consécutifs p, $p+2k$?

Q$_2$ Prenons deux nombres premiers p et q. Quelle est la valeur minimale de $|p-q|$ si on force p et q à être plus grands que N et qu'on fait croître N ?

Pour mettre la question **Q$_2$** en perspective il est bon de mentionner que puisqu'il y a $x/\ln x$ nombres premiers inférieurs ou égaux à x, alors la différence moyenne $|p-q|$ entre deux nombres premiers est de l'ordre de $\ln x$. Remarquons aussi que la valeur minimale de la question **Q$_2$** pourrait être infinie. Par contre, si on a une réponse à la question **Q$_1$**, alors on sait qu'il existe une valeur minimale finie inférieure ou égale à $2k$ pour la question **Q$_2$**.

Surprise ! Une fois qu'on a élargi nos questions on commence à voir : il y a eu beaucoup de progrès récents spectaculaires sur ces deux questions.

Le sujet a une longue histoire mais la première percée significative en 2009 est l'œuvre de l'équipe de Dan Goldston des États-Unis, Janos Pintz de Hongrie et Cem Yildirim de Turquie, qui a montré que si $p_1 = 2$, $p_2 = 3, \ldots$ sont les nombres premiers consécutifs, alors le rapport

$$\frac{p_{n+1}-p_n}{\ln p_n}$$

peut devenir arbitrairement petit (sur une certaine sous-suite des nombres premiers). Leur nouvelle méthode utilise la théorie des cribles d'une manière inattendue et donne des résultats bien meilleurs que ce que les chercheurs précédents avaient cru possible avec de telles techniques. Cela a stimulé la recherche sur la limite jusqu'où leurs idées pouvaient être poussées (en apportant des modifications et des ajouts appropriés à leur théorie).

Une réponse positive à la question Q$_1$

En 2013, la surprise a été encore plus grande : un mathématicien chinois de 57 ans, Yitang Zhang, qui n'avait publié qu'un seul article[4], a montré qu'il existe une infinité de paires de nombres premiers qui diffèrent de moins de 70 millions. Ceci donne une réponse positive à la question **Q$_1$**. En effet, supposons que pour chaque entier pair $2k < 7\times10^7$ il n'existe qu'un nombre fini de paires de nombres premiers p, $p+2k$. Comme on a un nombre fini d'entiers pairs positifs $2k < 7\times10^7$, ceci contredit le théorème de Zhang. Zhang n'a pas pu résoudre la conjecture des nombres premiers jumeaux, mais avec ce théorème, il montre qu'une conjecture analogue est vraie pour au moins un entier $2k$, bien qu'il n'ait pas pu identifier laquelle !

Comme c'est souvent le cas en mathématiques, les méthodes sont au moins aussi importantes que les résultats. Cette percée a ouvert la voie à de nouvelles méthodes et à une animation fébrile autour du sujet, si bien que le résultat de Zhang a été rapidement amélioré. En effet, Zhang a ajouté des

4. *Un professeur typique de son âge a publié entre 50 et 100 articles.*

James Maynard

James Maynard a fait son doctorat à Oxford en 2013. Après plusieurs postdocs, dont le premier au Centre de recherches mathématiques à Montréal, il est devenu professeur au Mathematical Institute d'Oxford en 2017.

James Maynard travaille sur la distribution des nombres premiers et, plus particulièrement sur les écarts entre nombres premiers. Dès son doctorat, à l'âge de 26 ans il a obtenu des résultats spectaculaires immédiatement célébrés dans le monde entier. Ses travaux lui ont valu de nombreux prix, dont un prix Erdös et le prix SASTRA Ramanujan en 2014, un prix Whitehead en 2015, un prix de l'European Mathematical Society en 2016, et le prix Cole en 2020. En 2022, sa recherche a été couronnée par la médaille Fields.

sophistications très profondes et difficiles aux idées de Goldston-Pintz-Yildirim. Donner une réponse positive à la question Q_1 avait semblé si improbable aux experts (comme moi) qu'il semblait inévitable que, pour progresser, on ait besoin d'autres idées vraiment profondes. Cette année-là, un jeune docteur en mathématiques d'Oxford, James Maynard, a rejoint notre groupe de recherche à l'Université de Montréal. Il voulait modifier différemment les outils de Goldston-Pintz-Yildirim, pour éviter la machinerie profonde utilisée par Zhang. Je lui ai dit qu'il était naïf. Il était peut-être naïf, mais il avait raison ! Quelques mois plus tard, il est revenu vers moi avec un argument correct qui fonctionnait et qui, techniquement, était encore plus simple que celui de Goldston-Pintz-Yildirim ![5]

À peu près à la même époque, Terence Tao, l'un des plus grands mathématiciens du monde et médaillé Fields en 2006, a proposé un argument similaire à celui de Maynard. En combinant leurs idées et en les poussant plus loin avec l'aide d'autres collaborateurs, ils ont pu montrer qu'il existe une infinité de paires de nombres premiers qui ne diffèrent pas de plus de 246. Ce n'est pas encore tout à fait la conjecture des nombres premiers jumeaux, mais on s'en rapproche beaucoup.

Maynard et Tao se sont également rendu compte que leurs preuves donnaient un grand résultat, allant bien au-delà de celui de Zhang :

Pour tout entier $m \geq 3$, il existe une infinité d'intervalles de longueur 2^{14m}, qui contiennent m nombres premiers. Autrement dit, il existe une infinité de m-tuples de nombres premiers consécutifs $p_n, p_{n+1}, \ldots, p_{n+m-1}$ tels que

$$p_{n+m-1} - p_n \leq 2^{14m}.$$

5. *L'explication de ces idées et leur développement est maintenant la plus grande source de thèses de maîtrise en théorie analytique des nombres.*

Il y a une effervescence en recherche pour découvrir d'autres propriétés des nombres premiers. Nous n'en regarderons que deux : une qui permet de construire une infinité de carrés magiques de nombres premiers, et de nouveaux résultats de James Maynard.

Des carrés et des cubes magiques de nombres premiers

Rappelons qu'un carré magique est une table $n \times n$ dont les sommes des entrées sur chaque ligne et chaque colonne et sur les deux diagonales sont toutes égales. En voici deux dont toutes les entrées sont des nombres premiers.

17	89	71
113	59	5
47	29	101

41	71	103	61
97	79	47	53
37	67	83	89
101	59	43	73

Comment les construit-on ? Le premier se construit en deux temps. On commence par construire un carré dont toutes les entrées sont des nombres premiers et dont chaque rangée et chaque colonne est une progression arithmétique et ensuite on réordonne les entrées des carrés.

Regardons le premier carré. On a réordonné les entrées de

5	17	29
47	59	71
89	101	113

Les rangées de ce nouveau carré sont de la forme p, $p+12$, $p+24$, et les colonnes, de la forme p, $p+42$, $p+84$. Si on numérote les rangées par $i \in \{0,1,2\}$ et les colonnes par $j \in \{0, 1, 2\}$, et qu'on regarde ce carré comme une matrice, son entrée $a_{i,j}$ est de la forme

$$a_{i,j} = 5 + 42i + 12j.$$

Cela fonctionne parce que les valeurs du polynôme de degré 1,

$$P(i, j) = 5 + 42i + 12j,$$

sont des nombres premiers pour $i, j \in \{0, 1, 2\}$.

L'étude des polynômes de degré 1,

$$P(i, j) = a + bi + cj \text{ où } a, b, c \in \mathbb{Z}$$

et dont les valeurs sont des entiers premiers pour $i, j \in \{0, 1, \ldots, k-1\}$ est un cas particulier de l'étude des polynômes

$$P(i_1, i_2, \ldots, i_k) = a_0 + a_1 i_1 + \ldots a_k i_k$$

pour lequels $P(i_1, i_2, \ldots, i_k)$ est premier pour $i_1, \ldots, i_k \in \{0, 1, \ldots, d-1\}$. C'est un champ de recherche important dans lequel Ben Green, Terence Tao et Tamar Ziegler ont obtenu de grands résultats depuis 2008. De tels polynômes permettent de construire des hypercubes de taille k^d dont les rangées dans les d directions sont des progressions arithmétiques de nombres premiers.

Une autre technique permet de construire le cube suivant (il faut voir les trois carrés comme trois couches d'un cube en dimension 3) dont les rangées dans les trois directions sont des progressions arithmétiques de nombres premiers :

251	419	587
167	263	359
83	107	131

149	401	653
173	347	521
197	293	389

47	383	719
179	431	683
311	479	647

Les nombres premiers avec décimales manquantes

En 2019, James Maynard s'est intéressé à une question sur laquelle se penchaient les mathématicien.ne.s depuis des siècles, soit les entiers n qui n'ont pas de chiffre 3 dans leur expansion décimale.

Parmi ceux-ci, y a-t-il une infinité qui sont premiers ?

Il y a 9 choix pour chaque chiffre de n (tous les entiers entre 0 et 9 sauf 3), et donc il y a 9^k entiers jusqu'à 10^k qui n'ont pas de 3 dans leur expansion décimale. On peut avoir l'impression qu'il y a beaucoup de tels nombres. Cette impression est fausse : il y en a peu. En effet, la proportion de tels nombres jusqu'à 10^k est $9^k/10^k = 0{,}9^k$, qui tend vers 0 quand k tend vers l'infini. Maynard a montré qu'il existe une infinité de tels nombres premiers et que, de plus, les nombres premiers ont une densité proche de $1/\ln(x)$ parmi tous les entiers sans décimale 3, soit exactement la même densité que celle des nombres premiers ! De plus, le même résultat est valable pour toute base ≥ 10 et tout chiffre manquant.

Comme vous le voyez, un résultat n'attend pas l'autre. Attendez-vous à de nouveaux développements dans les prochaines années !

La médaille Fields

La médaille Fields a été créée grâce à un legs de John Fields, autrefois titulaire de la chaire de mathématiques de l'université de Toronto. Elle est décernée par l'Union mathématique internationale depuis 1936. Elle est considérée comme le plus grand prix international pour la recherche mathématique, en quelque sorte le *prix Nobel des mathématiques*. La médaille Fields a été décernée à deux des mathématiciens dont nous avons parlé ici, Terence Tao et James Maynard, en grande partie pour ces travaux. Maynard a gagné la médaille en 2022 et garde des liens étroits avec Montréal où il collabore avec plusieurs chercheurs locaux.