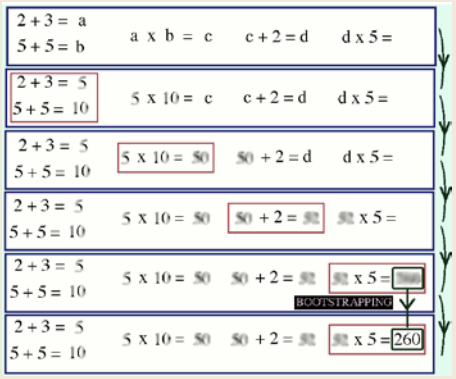
CALCUL FLOU ET *BOOTSTRAPPING*

Le système de calcul homomorphe initialement conçu par Craig Gentry se fonde sur deux idées que l'on retrouve dans tous les systèmes de calcul homomorphe inventés et perfectionnés depuis. La première idée est que les données doivent être chiffrées d'une manière floue, ce flou ne pouvant être effacé que par celui qui connaît la clé de déchiffrement. À mesure que les calculs homomorphes s'effectuent, le flou s'accroît – comme l'illustration ci-contre le symbolise. Après un certain nombre d'opérations, le flou devient si important que même avec la clé de déchiffrement, il est impossible d'accéder aux résultats. La seconde idée est qu'en s'y prenant bien (en demandant au système homomorphe d'exécuter l'opération de déchiffrement sur ses données, donc sans en prendre connaissance, et sans prendre connaissance des résultats), on réussit à effacer le flou qui risquait de devenir irrécupérable. C'est le *bootstrapping*, opération miraculeuse analogue à celle du baron de Münchhausen qui s'élevait dans les airs en tirant sur ses bottes. Soigneusement conçu et réalisé, ce nettoyage périodique des données est réellement possible et permet alors de mener des calculs homomorphes sans limitations de complexité : dès que le flou devient trop grand, on le réduit par *bootstrapping*.



un nombre limité d'opérations successives. Pour un calcul dépendant de plusieurs dizaines de bits b_1, b_2,..., b_k présents dans une expression complexe utilisant beaucoup de XOR et de ET, le résultat obtenu par l'opérateur extérieur risque d'être devenu illisible à celui qui lui a confié le calcul. La méthode sans le perfectionnement qui va venir ne fonctionne qu'avec des calculs assez limités. C'est là qu'intervient la deuxième idée majeure de Craig Gentry. Elle consiste à nettoyer périodiquement le bruit pour éviter qu'il ne devienne trop important.

Pour cela, on fait déchiffrer le résultat du calcul partiel avant qu'il ne soit trop brouillé. Ce nettoyage enlève tout le bruit. On l'effectue en demandant à l'opérateur extérieur d'appliquer la fonction de déchiffrement sur le résultat partiel, c'est-à-dire de diviser par p et examiner la parité du reste obtenu. Suprême astuce : puisqu'on ne fait pas confiance à l'opérateur extérieur, on ne lui communique pas la clé de déchiffrement (le nombre p), mais on lui demande de faire ce déchiffrement par un calcul homomorphe utilisant la méthode qu'on vient de décrire ! Ce n'est possible bien sûr que si ce calcul homomorphe du déchiffrement n'est pas trop complexe, c'est-à-dire n'exige pas, une fois traduit en XOR et en ET, une succession trop longue de calculs ; on s'en assurera.

Cela semble assez fou et cela ressemble à l'opération consistant à s'élever dans les airs en tirant sur ses bottes... c'est d'ailleurs pourquoi le nom donné à cette phase du calcul est *bootstrapping*. Pour que la phase de *bootstrapping* soit possible, il faut qu'un minimum d'opérations soient faisables sans que le bruit qui s'introduit soit devenu trop grand, et cela oblige à prendre des nombres entiers très longs pour p et les q_i, mais cela marche, et on dispose donc d'une méthode de calcul pleinement homomorphe comme on en rêvait. L'opération de *bootstrapping*, en nettoyant autant de fois que nécessaire les calculs partiels, rend possible des séries d'opérations aussi longues qu'on le souhaite de XOR et de ET ; et on peut donc faire exécuter tout calcul par un opérateur extérieur qui ignorera ce qu'il calcule.

Puisque la taille des bits chiffrés $\mathcal{C}(b)$ est nécessairement grande, les calculs effectués par l'opérateur extérieur sont très lourds, énormes comparés à ce qu'il faudrait faire si on ne souhaitait rien cacher, mais le but est atteint : on sait déléguer des calculs sans dévoiler ni les données ni le résultat.

ENCORE QUELQUES ORDRES DE GRANDEUR À GAGNER

Les travaux très nombreux sur ce sujet menés depuis 2009 ont visé à réduire les surcoûts en taille et en lourdeur de calcul des systèmes homomorphes. On progresse et des réalisations logicielles utilisant les idées mathématiques de ces travaux tentent de rendre les systèmes utilisables en pratique. La série d'opérations nécessaires au chiffrement de données par l'algorithme AES (Advanced Encryption Standard), très largement utilisé dans le monde entier, sert de repère pour mesurer les progrès des différents programmes de chiffrement homomorphe. On est ainsi passé, pour l'exécution de ce calcul test par un système homomorphe, de plusieurs heures (sur une machine courante) à quelques secondes.

C'est remarquable, mais pour que réellement on puisse envisager de confier massivement les calculs qu'on veut faire sur des données confidentielles à des opérateurs extérieurs qui les exécuteraient sans rien y voir, il faudra encore attendre un long moment, que le surcoût ait diminué de plusieurs ordres de grandeur. Certains experts tels que l'Américain Bruce Schneier restent réservés tant les surcoûts sont encore élevés. Aujourd'hui, la formidable idée de la cryptographie homomorphe est utile, par exemple pour la conception de systèmes de vote. Cependant, malgré une série d'idées intéressantes qui ont prouvé qu'elle était possible dans sa forme la plus générale, sa mise en œuvre pour tous, permettant plus de sécurité et une meilleure confidentialité sur les réseaux, devra encore attendre un peu. ■

BIBLIOGRAPHIE

X. YI *ET AL.*, *Homomorphic Encryption and Applications*, Springer, 2014.

V. CORTIER ET S. KREMER, Vote par Internet, *Interstices*, 2013. https://interstices.info/jcms/int_68258/vote-par-internet

M. VAN DIJK *ET AL.*, Fully homomorphic encryption over the integers, *Advances in cryptology* - EUROCRYPT 2010, Springer, pp. 24-43, 2010.

C. GENTRY, Fully homomorphic encryption using ideal lattices, *Proceedings of the 41st ACM Symposium on Theory of Computing*, pp. 169-178, 2009.

R. RIVEST *ET AL.*, *On data banks and privacy homomorphisms, Foundations of Secure Computation*, Academic Press, pp. 169-180, 1978.

L'ESSENTIEL

- Deux nombres premiers sont jumeaux, cousins ou sexy selon qu'ils sont respectivement séparés par 2, 4 ou 6.
- Combien y en a-t-il? Une infinité? Probablement, mais les mathématiciens ne savent pas encore le démontrer.
- Toutefois, on peut s'intéresser à leur régularité au sein des nombres entiers et étudier leur fréquence à partir de celle des nombres premiers.
- On se rapproche peut-être de la preuve tant attendue avec un résultat récent selon lequel il y a une infinité de paires de nombres premiers consécutifs distants d'au plus 246. Reste à remplacer ce 246 par 2...

L'AUTEUR

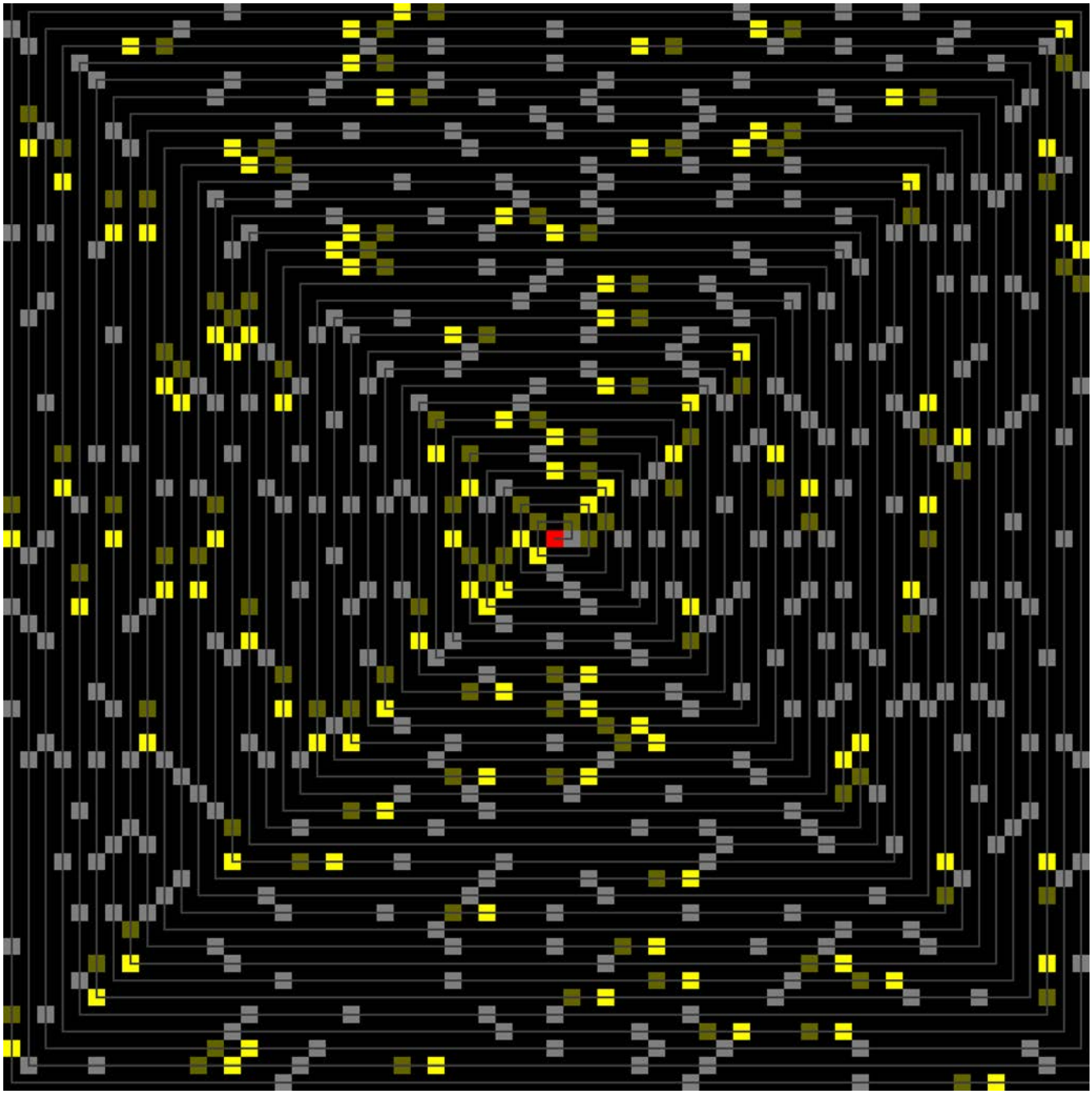
BRUNO MARTIN
Maître de conférences au laboratoire de recherche en Mathématiques de l'université du Littoral-Côte-d'Opale, à Calais.

Des jumeaux, des cousins et... des nombres sexy

La conjecture des nombres premiers jumeaux est l'un des problèmes non résolus les plus populaires en mathématiques. Des progrès extraordinaires ont été récemment accomplis, mais la route vers une démonstration est encore longue...

Petit exercice: recherchez tous les nombres premiers inférieurs à 60. Comment avez-vous procédé? Peut-être avez-vous testé pour chaque nombre s'il était divisible par un autre nombre que lui-même et 1, en faisant appel aux tables de multiplication ou même en utilisant une calculatrice? Cela fonctionne, mais c'est long! Une technique plus rapide est le crible d'Ératosthène. Elle consiste à éliminer, parmi tous les nombres, les multiples de 2, puis de 3, de 5... afin de ne conserver que les nombres premiers. On peut ensuite visualiser la disposition des nombres premiers au sein des nombres entiers de plusieurs manières, l'une des plus originales et surprenante étant la spirale d'Ulam (*voir l'encadré page 62*).

Grâce au crible ou tout autre moyen, listons les nombres premiers plus petits que 200: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197 et 199. Devant cette liste, on peut s'interroger: existe-t-il une règle permettant de passer d'un nombre premier au suivant? Par exemple, peut-on connaître le



Jean-Francois Colonna (CMAP/École Polytechnique, www.lactamme.polytechnique.fr)

Sur cette spirale d'Ulam le long de laquelle les entiers se suivent *(1, en rouge)*, les paires de nombres premiers jumeaux apparaissent en jaune *(sombre pour le premier de la paire, et vif pour le second)*.

nombre premier qui vient juste après 199 sans tester un par un les nombres qui suivent?

Au fait, est-on sûr qu'un nombre premier vient après 200? Rien *a priori* ne permet de l'affirmer. Bien sûr, en testant 201, 202, 203, 204... et on finit par ajouter 211 à la liste des nombres premiers. Le répit est de courte durée, car la question se repose immédiatement: y a-t-il un nombre premier après 211? Et ainsi de suite... En d'autres termes, la liste des nombres premiers s'arrête-t-elle à un moment donné?

UNE INFINITÉ DE PREMIERS

La réponse, certaine, est non. On sait prouver, depuis l'Antiquité, que la liste des nombres premiers est infinie. Le réservoir de nombres premiers est donc intarissable. Qu'en est-il alors d'une règle pour passer d'un nombre premier au suivant? Pour répondre, intéressons-nous à l'écart entre deux nombres premiers consécutifs, par exemple, celui entre 3 et 5 (2), entre 7 et 11 (4), et entre 53 et 59 (6). Cet écart obéit-il à des règles particulières?

À l'exception de 2, tous les nombres premiers sont impairs. Donc l'écart entre deux nombres premiers consécutifs est toujours un nombre pair, sauf bien sûr celui entre 2 et 3.

Et à part ça? Écrivons la liste des écarts successifs entre les nombres premiers consécutifs plus petits que 200: 1, 2, 2, 4, 2, 4, 2, 4, 6, 2, 6, 4, 2, 4, 6, 6, 2, 6, 4, 2, 6, 4, 6, 8, 4, 2, 2, 2, 4, 14, 4, 6, 8, 2, 10, 2, 6, 6, 4, 6, 6, 2, 10, 2, 4, 2... Aucune logique apparente. On remarque que l'écart le plus fréquent est 2 (il apparaît 16 fois), mais rien ne dit que cette prédominance se maintiendra lorsque l'on poursuivra >

> la liste. Et d'ailleurs, est-on certain de voir apparaître le nombre 2 une 17e fois ? une 18e ? et ainsi de suite ? Autrement dit : est-on certain de continuer inexorablement à rencontrer des nombres premiers consécutifs avec un écart de 2 comme 3 et 5, 5 et 7, 11 et 13, 17 et 19, 29 et 31, 41 et 43 ? De tels nombres sont des nombres premiers jumeaux. Nouvelle question : la liste des nombres premiers jumeaux s'arrête-t-elle ?

On l'ignore. Les mathématiciens penchent pour la négative, et misent sur une infinité de nombres premiers jumeaux, mais personne n'est en mesure d'en donner une preuve irréfutable ! Pourtant ce n'est pas faute d'avoir essayé. Si l'origine exacte de ce problème n'est pas certaine (la source la plus ancienne serait un article du mathématicien français Alphonse de Polignac écrit en 1849), on peut dire qu'il est l'objet de recherches intensives depuis plus de cent ans. C'est dire la difficulté !

Pour aborder ce problème, une première idée est de dire que nous ne sommes pas allés suffisamment loin dans l'expérimentation : nous n'avons observé que les nombres premiers jusqu'à 200. Avec un ordinateur, on peut aller bien au-delà et se faire une idée peut-être plus précise de l'évolution de la quantité de nombres premiers et des écarts entre nombres premiers consécutifs à mesure que l'on observe des nombres de plus en plus grands.

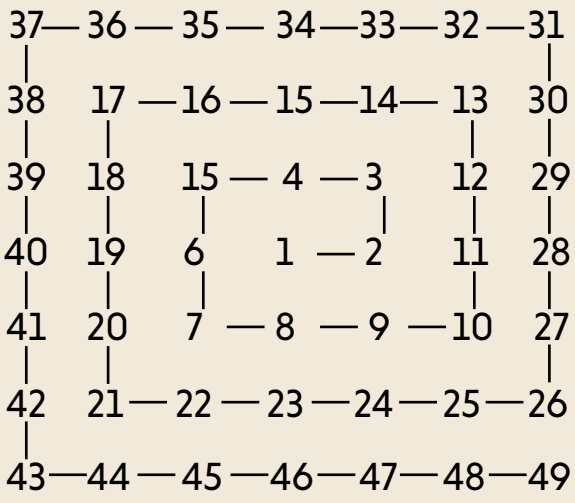
Une autre idée est d'examiner très attentivement les preuves connues de l'infinitude des nombres premiers, puis tenter d'adapter l'une de ces preuves pour en extraire des informations sur la liste des nombres premiers jumeaux.

Explorons d'abord la première piste, avec un ordinateur, pour aller au-delà de 200, par exemple jusqu'à 1 000 000. Les résultats : il y a 78 948 nombres premiers plus petits que 1 000 000. Et 8 169 paires de nombres premiers jumeaux parmi eux. C'est « beaucoup », mais ces chiffres seuls ne nous apprennent pas grand-chose. Il se pourrait par exemple que ces 78 948 nombres premiers soient tous situés entre 1 et 500 000 et qu'entre 500 000 et 1 000 000, il n'y en ait aucun, ce qui laisserait présager qu'au-delà de 500 000 il n'y a plus de nombres premiers.

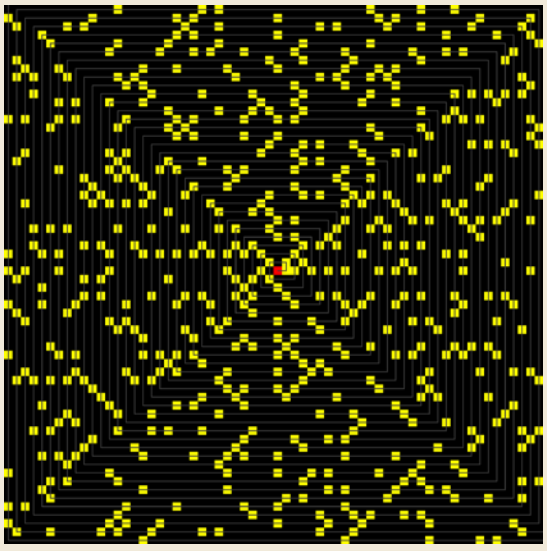
L'ESCALIER DES PREMIERS

Il est plus intéressant de suivre l'évolution de la quantité de nombres premiers rencontrés à mesure que nous progressons dans la suite des nombres entiers. Pour le visualiser, imaginons un promeneur qui avance sur un axe horizontal indexé par les nombres entiers. Dès qu'il tombe sur un nombre premier, il s'élève d'une marche, puis poursuit sa trajectoire à l'horizontale jusqu'à ce qu'il rencontre le nombre premier suivant. La hauteur à laquelle se trouve le promeneur

LA SPIRALE D'ULAM

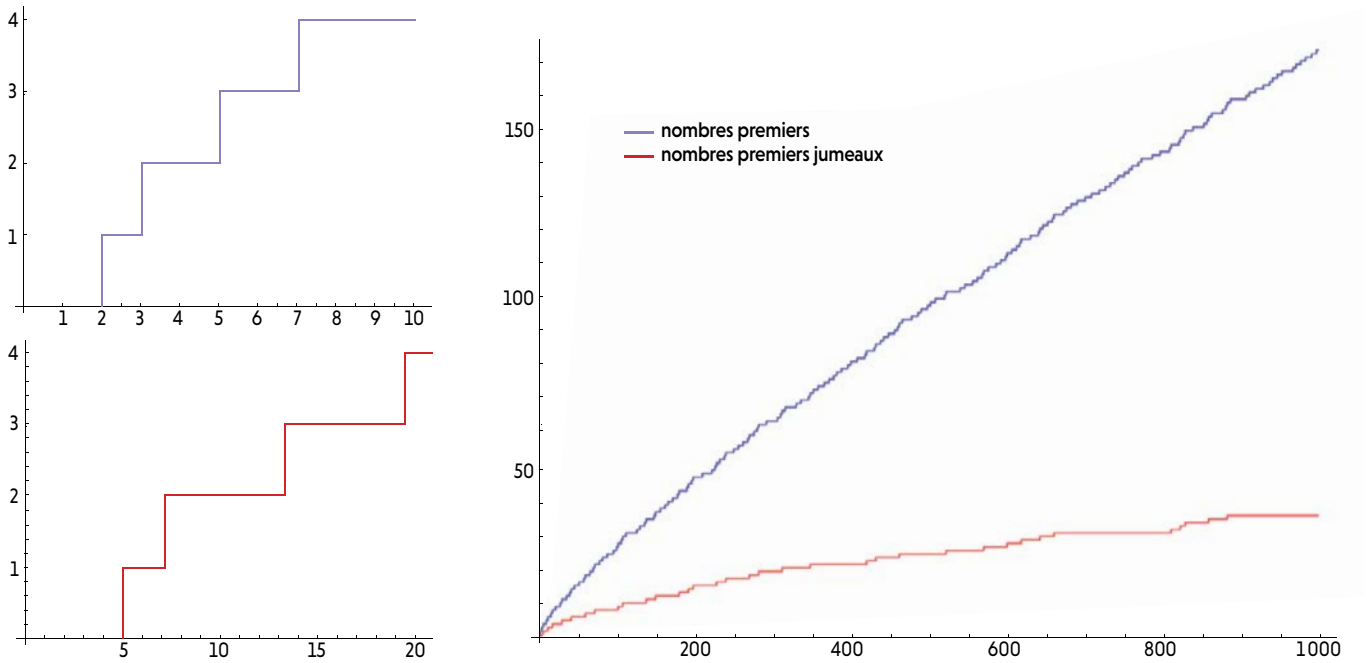


La légende raconte qu'un jour, s'ennuyant ferme lors d'une conférence, le mathématicien d'origine polonaise Stanisław Ulam, passa le temps en inscrivant sur un papier les entiers selon une spirale.



En entourant les nombres premiers, il eut la surprise de les voir s'aligner, pour certains, le long de diagonales. Il y aurait donc un semblant de régularité, partielle, dans la répartition des nombres premiers.

Jean-Françcois Colonna (CMAP/École polytechnique, www.lactamme.polytechnique.fr)



Les nombres premiers *(en bleu)* et les nombres premiers jumeaux *(en rouge)* semblent au départ progresser de façon erratique *(en haut)*, mais avec du recul *(en bas)*, on devine une certaine régularité.

correspond donc à la quantité de nombres premiers rencontrés depuis le début du parcours (*voir la figure ci-dessus*).

Au début (jusqu'à 10), les marches sont disposées de façon assez irrégulière, exactement comme le laisse prévoir la disposition d'apparence désordonnée des nombres premiers. Cependant, à mesure que l'on progresse vers 100, 1000... 1000000, et que l'on recule pour embrasser l'escalier du regard, l'ascension prend l'allure d'une courbe qui croît régulièrement et semble se confondre avec une droite: étonnant! Cela signifierait-il que la quantité de nombres premiers rencontrés évolue à une vitesse quasi constante? Y a-t-il autant de nombres premiers entre 1000 et 10000 qu'entre 10000 et 20000? entre 20000 et 30000?

Il n'en est rien. Voici quelques chiffres. On compte 1229 nombres premiers entre 1 et 10 000, 1033 entre 10000 et 20000, 983 entre 20000 et 30000, 958 entre 30000 et 40000. On devine un phénomène intrigant: on rencontre de moins en moins de nombres premiers. D'autres chiffres abondent dans ce sens. On croise 25 nombres premiers, soit 25%, entre 1 et 100, 170 (17%) entre 1 et 1000, 78498 (environ 7,8%) entre 1000 et 1000000...

La proportion de nombres premiers rencontrés semble donc diminuer progressivement à mesure que l'on parcourt la suite des nombres entiers. Autrement dit les nombres premiers semblent se raréfier! Chose extraordinaire, on sait démontrer que ce phénomène de raréfaction a bien lieu. Mieux, il peut être quantifié grâce à une célèbre fonction des mathématiques, le logarithme népérien noté ln, introduit dans un tout autre but par John Napier au XVII^{e} siècle. En effet, en mettant en œuvre des idées lumineuses exposées par Riemann en 1852, Hadamard et La Vallée-Poussin ont démontré indépendamment en 1896 qu'à mesure que x croît, le nombre de nombres premiers plus petits que x, souvent noté $\pi(x)$, tend à se comporter comme $x/\ln x$ (plus précisément, le rapport des deux tend vers 1). Ce magnifique résultat porte le nom de «Théorème des nombres premiers», il établit avec certitude que les nombres premiers se raréfient et précise à quelle vitesse. Étudier plus précisément l'écart entre $\pi(x)$ et $x/\ln(x)$ est une question fascinante et difficile, liée à l'un des problèmes ouverts les plus importants en mathématiques, connu sous le nom d'hypothèse de Riemann (*voir L'hypothèse qui valait un million, par P. Meier, page 68*).

Retenons en définitive que le nombre de nombres premiers progresse avec une certaine régularité, pour peu que l'on s'aventure vers des nombres suffisamment grands. La succession des nombres premiers paraissait imprévisible, et voilà qu'avec un peu de recul, la répartition des nombres premiers ne paraît plus si chaotique!

DU CÔTÉ DES JUMEAUX...

On peut s'intéresser aux nombres premiers jumeaux avec la même approche, celle de l'escalier où chaque marche correspond à une paire de nombres premiers jumeaux. Échauffons-nous doucement. Jusqu'à 20, le nouvel escalier s'est élevé de quatre marches, ce qui correspond aux quatre premières paires (3, 5), (5, 7), (11, 13) et (17, 19) de nombres premiers jumeaux.

À mesure que l'on parcourt les entiers, l'escalier des nombres premiers jumeaux semble davantage irrégulier que celui des nombres premiers (*voir la figure ci-dessus*). Il comporte >

quelques marches relativement longues, sortes de déserts de nombres premiers jumeaux. L'allure laisse même penser que le nombre de nombres premiers jumeaux ne va pas dépasser 50! Se dirige-t-on vers une extinction des nombres premiers jumeaux?

Non. En atteignant 1000000, on constate que l'escalier des nombres premiers jumeaux continue de s'élever, lentement mais apparemment sûrement. Il semble raisonnable de conjecturer que la liste des nombres premiers jumeaux ne s'arrête jamais. Et parmi les nombres premiers, quelle est la proportion de nombres premiers jumeaux? Et comment évolue cette proportion?

À l'instar des nombres premiers parmi les entiers, les nombres premiers jumeaux se raréfient au sein des nombres premiers. Qui plus est, ce comportement semble lui aussi relié à la fonction logarithme népérien. Seulement voilà, dans le cas des nombres premiers jumeaux, on ne dispose d'aucune démonstration à l'appui de ces observations. Rien ne nous permet de garantir que ces phénomènes (apparition de nombres premiers jumeaux, leur raréfaction...) perdurent indéfiniment.

... ET DES COUSINS SEXY

Nous en sommes venus à parler des nombres premiers jumeaux après avoir observé le caractère en apparence aléatoire des écarts entre nombres premiers successifs. Que se passe-t-il pour les nombres premiers consécutifs distants de 4 (les nombres premiers cousins)? de 6 (les nombres premiers sexy)? Ces deux listes sont-elles aussi infinies? Là encore, on pense que c'est le cas, mais le mystère plane tout autant.

On peut aussi se poser la question: y a-t-il plus de nombres premiers jumeaux ou de nombres premiers cousins, c'est-à-dire plus souvent des sauts de 2 ou de 4? Jusqu'à 1000, les escaliers correspondant aux nombres premiers jumeaux et aux nombres premiers cousins se dépassent mutuellement à plusieurs reprises (*voir la figure ci-dessous*). Ce phénomène de chevauchement se poursuit-il? Avec plus de marches (jusqu'à 1000000), les deux courbes semblent confondues! En zoomant, on observerait que les deux courbes semblent poursuivre ce jeu de dépassements successifs.

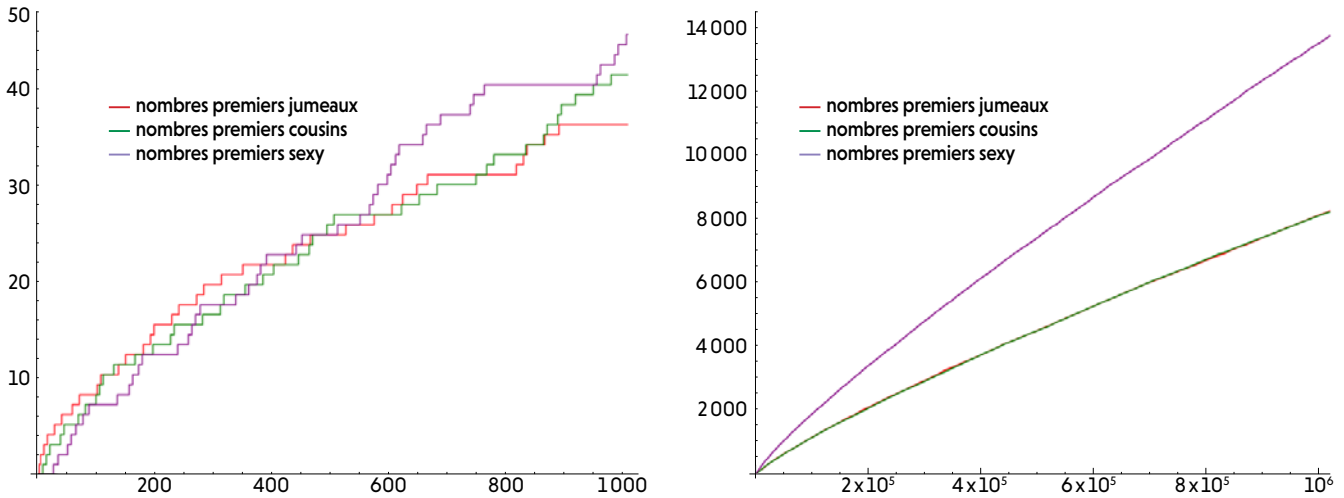
Qu'en est-il lorsque les nombres premiers sexy sont de la partie? Ils sont légèrement en tête à 1000 et s'imposent définitivement, et de manière très nette, au-delà. Entre les écarts 2, 4 et 6, ce dernier serait ainsi prépondérant. Nous pourrions poursuivre nos observations et multiplier les conjectures, sur la base de calculs numériques, en nous intéressant à tous les écarts possibles (tous les nombres pairs!). Privilégions plutôt un détour par les probabilités.

Dans ce domaine, les mathématiciens partent d'un constat audacieux: certes, la répartition des nombres premiers est parfaitement déterminée par leur définition, mais cette répartition n'est finalement pas si éloignée de ce que l'on obtiendrait en jouant à la loterie pour savoir quel nombre est premier.

Pas n'importe quelle loterie bien sûr! Le fonctionnement schématique est le suivant: on connaît la proportion de nombres premiers entre 1 et disons 1000000, soit environ 7,8%. Imaginez alors que pour chaque nombre, on tire à pile ou face pour décider son statut, premier ou pas, sachant que notre pièce est truquée de façon à donner pile dans seulement 7,8% des cas. Notre loterie est en fait un peu plus compliquée car on ne veut pas se limiter à 1000000, et elle fait intervenir le logarithme.

À partir de cette hypothèse d'apparence farfelue, les mathématiciens se livrent à des calculs de probabilité, relativement aisés, et aboutissent à des formules qui sont généralement en accord avec les expérimentations numériques: incroyable!

Pour résumer, tout se passe comme si les mathématiciens, partant d'une observation erronée, mais pas si éloignée de la réalité,



La progression relative des nombres premiers jumeaux *(en rouge)*, cousins *(en vert)* et sexy *(en violet)* semble incertaine au départ *(à gauche)*. Les choses s'éclaircissent *(à droite)*: les sexy l'emportent largement.

avaient construit une boule de cristal (on dit un modèle) permettant de réaliser des prédictions (ou des conjectures !) sur les nombres premiers, jumeaux, cousins… qui semblent fiables. Cette boule de cristal prédit par exemple qu'il y a une infinité de nombres jumeaux, qu'ils apparaissent régulièrement, et même qu'il finit par y avoir plus de nombres premiers sexy que de jumeaux. En revanche, elle reste muette quand à ces dépassements perpétuels entre cousins et jumeaux.

Pouvons-nous faire une confiance aveugle à cette boule de cristal ? Non, ces considérations probabilistes ne fournissent pas la moindre démonstration. Quel est leur intérêt en ce cas ? De nous aiguiller dans ce que l'on croit être la bonne direction, ce qui n'est pas rien. Il s'agit maintenant de construire les outils théoriques qui jetteront un pont entre probabilité et réalité ! Mais le gouffre qui sépare les deux semble infranchissable aujourd'hui, tout du moins pour la conjecture des nombres premiers jumeaux.

Nous avons précédemment conjecturé qu'il y a une infinité de paires de nombres jumeaux, une hypothèse que nous avons étayée par plusieurs graphiques. Mais la question reste entière : comment démontrer cette conjecture ? Commençons par oublier que ce problème est sans solution depuis près de deux siècles…

UN PROBLÈME « FACILE »

Une idée naturelle dans cette situation est de se mesurer à un autre problème, assez similaire mais plus simple. Puis, une fois le problème « facile » résolu, on cherche à modifier adéquatement la solution pour qu'elle s'applique au problème de départ. Ici le problème « facile » est tout trouvé : sait-on démontrer que la liste de tous les nombres premiers ne s'arrête jamais ?

Mais avant même d'attaquer la première étape – bien comprendre une preuve du fait qu'il y a une infinité de nombres premiers –, concentrons-nous sur la notion délicate d'infinité. Comment démontrer que la liste d'une certaine famille de nombres ne s'arrête jamais ?

Partons d'une situation familière. Les enfants demandent souvent : « Quel est le plus grand nombre ? » « Il n'y en a pas, car ça ne s'arrête jamais », leur répond-on, et c'est souvent le début d'une réflexion silencieuse ou d'une avalanche de questions. Un moyen de les convaincre est d'ajouter : « Prends n'importe quel nombre. Tu peux toujours ajouter 1 pour obtenir un nombre plus grand. »

Avec cette « recette » (ajouter 1), on fabrique une infinité de nombres. Grâce à cette technique, on peut prouver que certaines familles de nombres sont de taille infinie, comme celle des nombres impairs avec, par exemple, la recette : prenez un nombre impair et ajoutez 2. Peut-on trouver une recette de ce genre pour prouver que la liste des nombres premiers ne s'arrête pas ? C'est difficile.

LA RECETTE D'EUCLIDE

Le mathématicien grec Euclide en a le premier trouvé une satisfaisante, qu'il a consignée dans son traité *Les Éléments*, vers 300 avant notre ère. La recette est astucieuse et nécessite quelques efforts. Mais le résultat en vaut la chandelle !

Nous allons avoir l'usage d'une propriété toute simple : deux nombres consécutifs n'ont qu'un seul diviseur en commun, le nombre 1. Par exemple, 99 et 100 ont pour diviseurs respectifs (1, 3, 11, 33, 99) et (1, 2, 4, 5, 10, 20, 25, 50, 100). On le démontre ainsi. Prenez deux nombres consécutifs et considérez un nombre qui les divise tous les deux. Il divisera aussi leur différence. Or cette différence vaut 1. Donc ce diviseur commun aux deux nombres de départ divise 1, ce qui nous laisse peu de doutes sur son identité : ce diviseur vaut 1.

Au-delà de 1 000, les nombres sexy s'imposent définitivement face aux nombres jumeaux et cousins

Une autre propriété cruciale est que tout nombre est divisible par (au moins) un nombre premier. Ce sera la clé de voûte de la preuve d'Euclide. Quelques exemples vont guider notre démonstration. La liste des diviseurs de 45 est (1, 3, 5, 9, 15, 45), parmi lesquels 3 et 5 sont premiers. La liste des diviseurs de 61 est (1, 61) : c'est un nombre premier. La liste des diviseurs de 32 est (1, 2, 4, 8, 16, 32) et 2 est bien un nombre premier.

La démonstration repose sur l'observation suivante : si l'on dresse la liste des diviseurs strictement plus grands que 1 d'un nombre, le plus petit d'entre eux est toujours un nombre premier, les exemples précédents en attestent. Imaginons que ce plus petit >

> diviseur, notons-le *n° 1*, ne soit pas premier. Puisqu'il n'est pas premier, *n° 1* est donc divisible par un nombre, *n° 2*, strictement plus petit que *n° 1* et strictement plus grand que 1. Mais ce *n° 2* divise *n° 1* qui lui-même divise le nombre de départ. Donc *n° 2* divise le nombre de départ. Voilà qui est gênant : deux nombres différents se disputent la place de plus petit diviseur du nombre de départ. Notre hypothèse de départ (le plus petit diviseur n'est pas premier) ne tient pas la route : ce plus petit diviseur est forcément premier.

Nous sommes maintenant en mesure de donner cette recette d'Euclide qui montre que la liste des nombres premiers est inépuisable. Prenons un exemple avec les nombres premiers 2, 3 et 5, et formons le produit 2×3×5 (sans effectuer le calcul). Ce nombre est divisible par 2, 3 et 5. Maintenant ajoutons 1 : 2×3×5+1. Les deux nombres 2×3×5 et 2×3×5+1 sont bien consécutifs. D'après la première propriété, ils n'ont donc aucun diviseur en commun si ce n'est 1. Le nombre 2×3×5+1 n'est donc divisible ni par 2, ni par 3, ni par 5. Pourtant la deuxième propriété nous dit qu'il possède un diviseur qui est un nombre premier. Nous venons de montrer qu'il se trouve un nombre premier qui est différent de 2, 3 et 5. Inutile de savoir de quel nombre il s'agit : il existe et il est différent des nombres premiers 2, 3, 5 déjà connus, c'est tout ce que l'on voulait.

Voici donc une recette de fabrication d'un nouveau nombre premier à partir de plusieurs autres : prenez plusieurs nombres premiers, multipliez-les entre eux, ajoutez 1 au résultat et vous obtenez un nombre divisible par un nouveau nombre premier différent de ceux du départ. Avec cette recette, la liste des nombres premiers pourra toujours être agrandie : il y a une infinité de nombres premiers.

LE PROBLÈME RESTE ENTIER

La première étape de notre plan, résoudre un problème « facile » est franchie. Passons à la deuxième. Peut-on s'inspirer de cette recette de fabrication de nombres premiers pour en former une qui produise des nombres premiers jumeaux ? Peut-être, mais jusqu'à présent personne n'y est parvenu. Et l'on ignore toujours s'il y a une infinité de nombres premiers jumeaux.

Après Euclide, d'autres mathématiciens ont produit de nouvelles démonstrations du fait qu'il y a une infinité de nombres premiers. Des chercheurs très inventifs s'en sont inspirés pour essayer de prouver qu'il existe une infinité de nombres premiers jumeaux. Cela a débouché sur la construction de théories mathématiques incroyablement élaborées qui n'ont pourtant pas encore permis de résoudre ce problème.

Néanmoins on s'en rapproche… la preuve avec un résultat récent obtenu par les efforts conjoints de plusieurs chercheurs. Prenez la liste des nombres premiers jumeaux, celle des nombres premiers cousins, celle des sexy et regroupez-les dans une même liste. On n'est pas encore capable de montrer que cette nouvelle liste ne s'arrête pas. Ajoutez les nombres premiers consécutifs distants de 8, puis ceux de 10, puis ceux de 12… jusqu'à ajouter les nombres premiers consécutifs distants de 246. Et bien la liste ainsi obtenue ne se termine pas, on sait maintenant le prouver !

DE 70 000 000 À 246

De façon synthétique, on peut dire qu'il y a une infinité de paires de nombres premiers consécutifs distants d'au plus 246. Ce résultat peut paraître curieux, et peu élégant. Il est pourtant qualifié d'extraordinaire par les experts des nombres premiers. En fait, il y a encore six ans, personne n'était capable de prouver un résultat de ce type, même en remplaçant 246 par un entier N beaucoup plus grand.

Pourquoi 246 ? Dans un premier temps, en 2013, le mathématicien chinois Yitang Zhang a établi le résultat pour N = 70 000 000 qui a stupéfait et passionné la communauté mathématique. Pouvait-on améliorer la preuve d'Yitang Zhang et remplacer 70 000 000 par un nombre bien plus petit ? Plusieurs chercheurs se sont lancés dans l'aventure et ont entamé une collaboration intensive *via* un forum public de discussion sur Internet. Cette pratique, relativement neuve dans le milieu, avait été conceptualisée et lancée par le mathématicien anglais Tim Gowers sous le nom de *Polymaths*. Chaque projet *Polymath* réunit virtuellement un groupe plus ou moins important de chercheurs intéressés autour d'un problème ouvert bien précis, et pour un laps de temps plus ou moins long. Toute publication qui en résulte est signée sous le pseudonyme collectif D. H. J. Polymath.

Après une succession d'améliorations, une nouvelle percée du jeune mathématicien anglais James Maynard, puis de nouvelles améliorations, le projet *Polymath n° 8* parvint à ce fameux 246. Mais même avec ces progrès extraordinaires, établir la conjecture des nombres premiers jumeaux (ce qui en somme consisterait à remplacer ce 246 par 2) semble hors d'atteinte actuellement aux dires des spécialistes.

Le chemin qui mène à une démonstration de cette conjecture semble donc encore bien long. Et pire encore, une telle preuve, si elle venait à être trouvée, resterait probablement incompréhensible à toute personne n'ayant pas un solide bagage mathématique. Alors que vous veniez juste de vous attaquer au problème avec un papier et un crayon… ■

Cet article est adapté de celui paru sur le site du CNRS *Images des Mathématiques* : http://images.math.cnrs.fr/
Nous en remercions les équipes de nous avoir autorisé à le reproduire.

BIBLIOGRAPHIE

J.-P. DELAHAYE, *Merveilleux nombres premiers. Voyage au cœur de l'arithmétique*, Belin, 2013.

M. DU SAUTOY, *La symphonie des nombres premiers*, Seuil, 2007

J. DERBYSHIRE, *Dans la jungle des nombres premiers*, Dunod, 2007.

POUR LA SCIENCE
Édition française de Scientific American

HORS-SÉRIE

COMPLÉTEZ VOTRE COLLECTION DÈS MAINTENANT !

N° 91 (avr. 16)
réf. DO091

N° 92 (juil. 16)
réf. DO092

N° 93 (oct. 16)
réf. DO093

N° 94 (janv. 17)
réf. DO094

N° 95 (avr. 17)
réf. DO095

N° 96 (août 17)
réf. DO096

N° 97 (nov. 17)
réf. DO097

N° 98 (févr. 18)
réf. DO098

N° 99 (mai 18)
réf. DO099

N° 100 (août 18)
réf. DO100

N° 101 (nov. 18)
réf. DO101

N° 102 (fév. 19)
réf. DO102

RETROUVEZ L'ENSEMBLE DES ANCIENS NUMÉROS SUR **BOUTIQUE.POURLASCIENCE.FR/HORS-SERIE.HTML**

À retourner accompagné de votre règlement à :
Pour la Science – Service VPC – 19 rue de l'Industrie – BP 90053 – 67402 Illkirch Cedex – email : pourlascience@abopress.fr

☑ **OUI, je commande des numéros de Pour la Science Hors-série, au tarif unitaire de 10,90 €.**

1 / JE REPORTE CI-DESSOUS LES RÉFÉRENCES à 5 chiffres correspondant aux numéros commandés :

1re réf. ..... 0 1 x 10,90 € = 1 0 9 0 €
2e réf. ..... x 10,90 € = €
3e réf. ..... x 10,90 € = €
4e réf. ..... x 10,90 € = €
5e réf. ..... x 10,90 € = €
6e réf. ..... x 10,90 € = €

TOTAL À RÉGLER €

Offre valable jusqu'au 31/12/2019 en France Métropolitaine. Pour une livraison à l'étranger, merci de consulter **boutique.pourlascience.fr**

Les informations que nous collectons dans ce bon de commande nous aident à personnaliser et à améliorer les services que nous vous proposons. Nous les utiliserons pour gérer votre accès à l'intégralité de nos services, traiter vos commandes et paiements, et vous faire part notamment par newsletters de nos offres commerciales moyennant le respect de vos choix en la matière. Le responsable du traitement est la société *Pour La Science*. Vos données personnelles ne seront pas conservées au-delà de la durée nécessaire à la finalité de leur traitement. *Pour la Science* ne commercialise ni ne loue vos données à caractère personnel à des tiers. Les données collectées sont exclusivement destinées à *Pour la Science*. Nous vous invitons à prendre connaissance de notre charte de protection des données personnelles à l'adresse suivante : https://rebrand.ly/charte-donnees-pls Conformément à la réglementation applicable (et notamment au Règlement 2016/679/UE dit « RGPD ») vous disposez des droits d'accès, de rectification, d'opposition, d'effacement, à la portabilité et à la limitation de vos données personnelles. Pour exercer ces droits (ou nous poser toute question concernant le traitement de vos données personnelles), vous pouvez nous contacter par courriel à l'adresse protection-donnees@pourlascience.fr.

2 / J'INDIQUE MES COORDONNÉES

☐ M. ☐ Mme
Nom : .....
Prénom : .....
Adresse : .....
.....
Code postal ..... Ville : .....
Téléphone .....
J'accepte de recevoir les offres de Pour la Science ☐ OUI ☐ NON

3 / JE CHOISIS MON MODE DE RÈGLEMENT

☐ **Par chèque à l'ordre de** *Pour la Science*
☐ **Carte bancaire**
N° .....
Date d'expiration .....
Clé (les 3 chiffres au dos de votre CB) .....

Signature obligatoire :

Groupe Pour la Science – Siège social : 170 bis, boulevard du Montparnasse, CS20012, 75680 Paris Cedex 14 – Sarl au capital de 32000 € – RCS Paris B 311 797 393 – Siret : 311 797 393 000 23 – APE 5814 Z

PLUS SIMPLE, PLUS RAPIDE
ABONNEZ-VOUS SUR BOUTIQUE.POURLASCIENCE.FR