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.