

> 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.

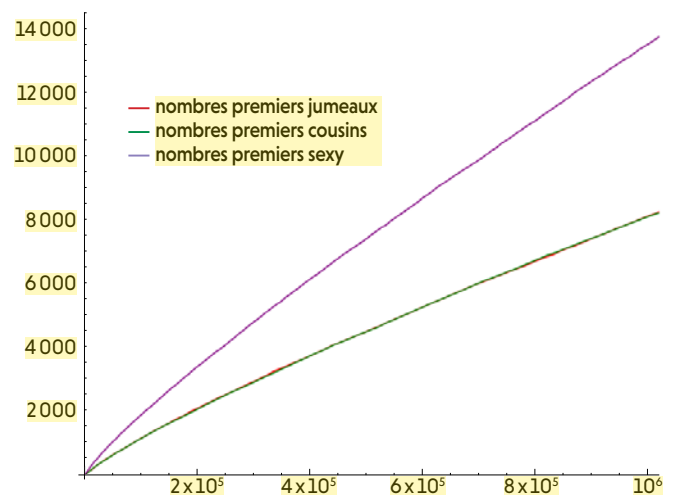
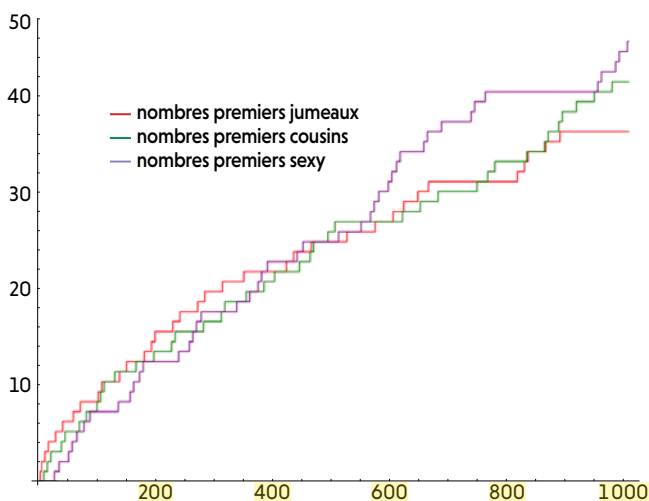
Dans ce domaine, les mathématiciens partent d'un constat audacieux: certes, la répartition des nombres premiers est parfaitement déterminée par leur définition, mais cette répartition n'est finalement pas si éloignée de ce que l'on obtiendrait en jouant à la loterie pour savoir quel nombre est premier.

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

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

divise 1, ce qui nous laisse peu de doutes sur son identité: ce diviseur vaut 1.

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