3. NOMBRES PREMIERS JUMEAUX, COUSINS ET SEXY : LA CONJECTURE DE POLIGNAC

Deux nombres premiers jumeaux sont écartés de 2, comme 11 et 13. Deux nombres premiers cousins sont écartés de 4 (comme 7–11 ou 13–17). S'ils sont écartés de 6 (comme 5–11, 7–13, 11–17, 13–19, 23–29 ou 31–37), ce sont des nombres premiers «sexy». On conjecture qu'il y a une infinité de nombres premiers cousins et de nombres premiers sexy. Plus généralement, on examine les paires de nombres premiers dont l'écart est $2k$. La conjecture de Polignac est que, pour chaque k positif, il existe une infinité de ces paires.

Hardy et Littlewood, armés d'arguments heuristiques, ont précisé la conjecture : si on note $\pi_d(m)$, le nombre de paires de nombres premiers dont l'écart est d alors :

$$\pi_d(m) \approx 2\, C_j \frac{m}{(\log m)^2} \prod_{p|d\ p>2} \frac{(p-1)}{(p-2)}$$

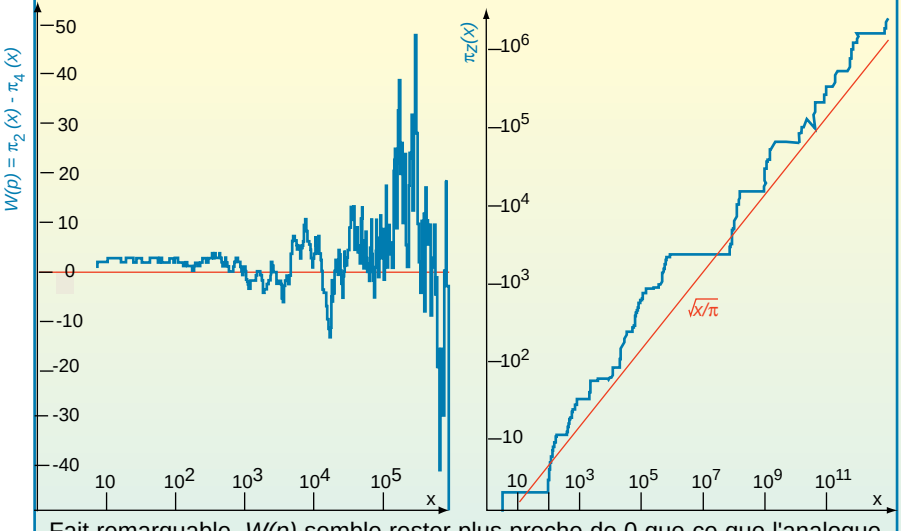
avec C_j = 0,6601618158468... constante des nombres premiers jumeaux

$$C_j = (1-1/2^2)(1-1/4^2)(1-1/6^2)(1-1/10^2)... = \prod_{\text{premier}>2} \left(1-\frac{1}{(p-1)^2}\right)$$

Pour d = 2 et d = 4, le produit vaut 1. Pour d = 6, il vaut 2. Cela signifierait (si la conjecture est juste) qu'il existerait autant de nombres premiers jumeaux que de nombres premiers cousins et deux fois plus de nombres premiers sexy. Ces prédictions sont remarquablement en accord avec ce qu'on obtient, par exemple, en menant un décompte pour $n = 10^8$:

$\pi_2(10^8)$ = 440312 $\pi_4(10^8)$ = 440258 $\pi_6(10^8)$ = 879908, voisines des valeurs données par les formules de Hardy et Littlewood : 440368, 440368 et 880736.

Récemment, M. Wolf s'est intéressé à la fonction $W(p)$ donnant la différence entre le nombre de nombres premiers jumeaux inférieurs à p et le nombre de nombres premiers cousins inférieurs à p : $W(p) = \pi_2(p) - \pi_4(p)$. Le graphe de cette fonction présente l'aspect d'une fractale dont la dimension a été évaluée à 1,48, valeur proche de celle que l'on trouve pour un mouvement brownien.



Fait remarquable, $W(p)$ semble rester plus proche de 0 que ce que l'analogue de la conjecture de Riemann pour les nombres premiers, jumeaux ou cousins laissait attendre. C'est une régularité inattendue dans le comportement des nombres premiers.

L'étude des nombres premiers p pour lesquels $W(p)$ = 0 (valeur pour laquelle le nombre de nombres premiers jumeaux est exactement le même que le nombre de nombres premiers cousins) et la comparaison avec une marche aléatoire ont conduit M. Wolf à la conjecture que cette égalisation se produit environ $\sqrt{p}/\pi$ fois entre 0 et p. Le dessin de la courbe $\pi_Z(p)$ qui compte ces nombres premiers entre 0 et p confirme la conjecture. Là encore, il s'agit d'une régularité inattendue dans le comportement des nombres premiers.

Les graphiques sont repris de l'article de M. Wolf : *On Twin and Cousin Primes.*

ment (c'est ce qui s'est passé avec le théorème de Fermat).

DES DÉBUTS DE PREUVES?

Une façon indirecte de formuler la conjecture des nombres premiers jumeaux consiste à l'énoncer sous la forme : «Le nombre 2 peut s'écrire d'une infinité de façons différentes sous la forme $p_1 - p_2$, p_1 et p_2 étant des nombres premiers.»

Des résultats très sérieux qui approchent cet énoncé ont été prouvés en utilisant la technique des cribles (qui généralise l'idée du crible d'Ératosthène). En 1920, Viggo Brun a ainsi démontré que le nombre 2 peut s'écrire d'une infinité de façons différentes sous la forme $p_1 - p_2$, les nombres p_1 et p_2 étant des nombres «9-presque-premiers», dont nous allons donner la définition : un nombre «k-presque-premier» est un nombre dont la décomposition en facteurs premiers a k facteurs au plus. Ainsi le nombre 169 égal à 13×13 est 2-presque-premier et 12 égal à $2\times2\times3$ est 3-presque-premier.

Le résultat de V. Brun est très loin du but qui sera atteint quand on aura remplacé «9-presque-premiers» par «1 presque-premiers», puisque bien sûr «être 1-presque-premier» équivaut à «être premier». Cependant les progrès ont été continus : en 1924, H. Rademacher a remplacé le 9 par 7, et, à la suite de travaux de A. Rényi en 1947 et de J. Chen en 1966, on sait maintenant que le nombre 2 s'écrit d'une infinité de façons différentes sous la forme $p_1 - p_2$ avec p_1 premier et p_2 un nombre 2-presque-premier. Ainsi, nous nous rapprochons : il n'y a plus qu'à remplacer 2-presque-premier par 1-presque-premier!

CONSTANTE DE V. BRUN

L'étude de la raréfaction des nombres premiers jumeaux fait intervenir la série des inverses des nombres premiers jumeaux. En 1919, le mathématicien V. Brun prouva que la série des inverses des nombres premiers jumeaux était convergente. Contrairement à la série des inverses des nombres premiers (1/2 + 1/3 + 1/5 + 1/7 + 1/11 + ...), qui devient infinie quand on augmente le nombre des termes, la série des inverses de nombres premiers jumeaux, égale à : (1/3+1/5) + (1/5+1/7) + (1/11+1/19) + (1/29+1/31) + .., est de valeur finie. Remarquez que l'on fait apparaître deux fois 1/5, le second élément de la paire 3-5 en même temps que le premier de la paire 5-7.

Le fait que la série ait une valeur finie signifie qu'il y a infiniment moins de nombres premiers jumeaux que de nombres premiers. En effet, si, en moyenne, un nombre premier sur 100 était

un nombre premier jumeau, alors la série des inverses des nombres premiers jumeaux serait infinie, comme la série des inverses de nombres premiers (car l'infini divisé par 100 est encore l'infini). Donc moins d'un nombre premier sur 100 est un nombre premier jumeau. Ce qui vient d'être dit pour 100 peut être répété avec 1 000, 10 000, etc. Il y a bien raréfaction : en allant assez loin, la proportion des nombres premiers jumeaux parmi les nombres premiers tend vers 0.

Il résulte qu'il y a des séquences de plus en plus longues de nombres premiers consécutifs ne comportant aucun nombre premier jumeau. Ce résultat est à rapprocher de celui qui énonce qu'il y a des séquences de nombres composés successifs aussi longues qu'on veut : en effet, par exemple, il n'y a aucun nombre premier entre $N!+2$ et $N!+N$ (en effet, $N!+2$ est multiple de 2 ; $N!+3$ multiple de 3 ; etc.).

Que la série des inverses des premiers jumeaux converge est intéressant, mais cela n'indique évidemment pas qu'il y a nécessairement une infinité de nombres premiers jumeaux : la série peut avoir une valeur finie parce que le nombre de ses termes est fini, ou parce qu'ils sont de plus en plus petits. La valeur de la série $(1/3 + 1/5) + (1/5 + 1/7) + (1/11 + 1/19) + \ldots$ se dénomme *B*, la constante de V. Brun.

Cette constante *B* est particulièrement difficile à évaluer, et l'on ne connaît pas d'autres méthodes pour la calculer que d'utiliser directement sa définition : il faut donc aller très loin dans le calcul des nombres premiers.

La constante de V. Brun a été estimée par Daniel Shanks et John Wrench en 1974 (qui furent aussi les premiers à calculer 100 000 décimales du nombre π, en 1961), puis par Richard Brent en 1976. Le calcul de D. Shanks et J. Wrench utilisa les deux premiers millions de nombres premiers ; celui de R. Brent prit en considération les nombres jusqu'à 100 milliards (ils dénombrèrent 224 376 048 nombres premiers jumeaux). Plus récemment, le calcul a été poussé plus avant par M. Kutrib et J. Richstein, et indépendamment par Thomas Nicely, ce dernier étant au centre d'une aventure dont le récit va nous plonger dans le monde des erreurs informatiques.

Thomas Nicely et le Pentium d'Intel

T. Nicely est professeur au Lynchburg College, en Virginie, aux États-Unis. Il mène des recherches en théorie «computationnelle» des nombres et s'intéresse particulièrement aux nombres premiers. Souhaitant améliorer la précision de la constante de V. Brun, il lança en 1994 une série de calculs fondée sur l'énumération des nombres premiers et des nombres premiers jumeaux inférieurs à 10^{15}. À cause du coût des mémoires informatiques (il en faut énormément pour aller jusqu'à 10^{15}), son calcul se déroulait par tranches ; quand il passait d'une tranche à la suivante, il effaçait les nombres premiers calculés après en avoir extrait les informations qui l'intéressaient (il est plus facile de calculer des nombres premiers que de les stocker !). La séparation en tranches lui a permis aussi de répartir son calcul sur de nombreux ordinateurs qu'il faisait travailler pour lui dès que leurs propriétaires les laissaient inoccupés (technique qui est devenue classique pour mener de longs calculs).

De façon à garantir les résultats, T. Nicely, comme il est d'usage dans ces domaines, effectuait de nombreux contrôles : calculs effectués plusieurs fois, recoupements de méthodes indépendantes, etc. Notons que, dans l'absolu, même après contrôles, nul ne peut exclure qu'il subsiste encore une erreur. Il se peut, par exemple, que deux erreurs dans deux calculs différents produisent le même résultat... erroné. Cette possibilité est cependant jugée très improbable, et l'on néglige une telle éventualité. Comme toujours en sciences expérimentales, la probabilité d'erreur peut être rendue faible, voire très faible, mais jamais totalement nulle.

Lors de son calcul, T. Nicely, à sa grande déception, trouva une anomalie. Quelque chose clochait, car deux résultats qui auraient dû coïncider étaient différents. Dans un tel cas (fréquent !), le programmeur commence par soupçonner *(a)* le programme, puis, dans l'ordre, *(b)* le compilateur ; *(c)* d'éventuels virus ; *(d)* le système d'exploitation et seulement enfin *(e)* le matériel : mémoires, bus de données ou microprocesseur. On n'en arrive pratiquement jamais à l'étape *(e)*, car on a trouvé l'erreur avant ou, assez fréquemment, elle a disparu quand on a modifié le programme sans que personne ne comprenne bien pourquoi ! Les causes matérielles peuvent être particulières à votre machine (saleté sur un de vos circuits, composants défectueux) ou générales : erreur dans la conception ou le dessin d'un circuit. L'erreur aléatoire provoquée par un rayon cosmique inopportun ou une charge électrique parasite qui fait basculer un circuit ne sont pas à exclure, mais elles sont quasi impossibles à diagnostiquer rétrospectivement.

L'anomalie décelée par T. Nicely refusait de disparaître : aucune des causes simples envisagées ne semblait responsable. Après plusieurs semaines de recherche durant lesquelles T. Nicely avait fait exécuter la partie du programme d'où semblait provenir l'erreur sur un processeur plus ancien (un 486 d'*Intel*), il assista interloqué à sa disparition. En décortiquant alors de près sa découverte, il aboutit (quatre mois après la détection de l'erreur) à la certitude que c'était le *Pentium* d'*Intel* qui était la cause du mal. Celui-ci évaluait faussement l'inverse des nombres premiers jumeaux : 824 633 702 441 et 824 633 702 443, l'évaluation étant fausse dès le dixième chiffre !

Après avoir averti la Société *Intel*, qui ne répondit pas, il informa ses collègues de l'erreur et la nouvelle se répandit dans le monde entier comme une traînée de poudre, obligeant *Intel* à réagir. *Intel* reconnut avoir eu connaissance de l'erreur, mais ne pouvait échanger toutes les puces défectueuses (plus de cinq millions en avaient été vendues, et même le puissant *Intel* n'aurait pu supporter le coût d'un remplacement systématique). Seuls les acheteurs pouvant attester que le type d'erreurs détectées dans certaines divisions étaient graves pour eux purent obtenir la puce de remplacement (quand elle fut rendue disponible). Il en résulte que la puce de nombreux ordinateurs encore en service (fabriqués en 1994 et

4. LES CONSTELLATIONS

À l'exception de 3, 5, 7, trois nombres premiers consécutifs ne peuvent être de la forme $[p, p+2, p+4]$; en revanche, $[p, p+2, p+6]$ et $[p, p+4, p+6]$ sont des formes possibles pour trois nombres premiers consécutifs. Pour quatre nombres premiers, $[p, p+2, p+6, p+8]$ est possible. C'est ce que l'on dénomme les constellations, et l'on conjecture que, pour chacune, il y a une infinité de nombres premiers.

Hardy et Littlewood ont donné une version numérique de la conjecture des constellations qui précise leur densité. Cette conjecture semble numériquement vérifiée.

Les trois plus grands triplets-premiers connus, tous découverts en 1998, sont :

$34344713643960930(2^{3567}-2^{1189})-6\times2^{1189}-7,-5,-1$ (1091 chiffres, T. Forbes)

$23873826365759390(2^{3567}-2^{1189})-6\times2^{1189}-5,-1,+1$ (1091 chiffres, T. Forbes)

$20834081158360750(2^{3567}-2^{1189})-6\times2^{1189}-5,-1,+1$(1091 chiffres, T. Forbes)

Le site Internet de Tony Forbes, http://www.ltkz.demon.co.uk/ktuplets.htm donne les mises à jour des records actuels pour les constellations, les triplets, les quadruplets, etc.