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.

1995) reste défectueuse *(voir la figure 1, qui vous permet de savoir si vous êtes concerné)*. Si cette imperfection est sans importance pour faire courir et sauter Lara Croft ou pour le bon fonctionnement d'un traitement de texte, il n'en est pas ainsi pour ceux qui utilisent un tableur ou un logiciel de statistiques.

L'argument avancé par *Intel* que l'erreur ne se produit qu'une fois tous les 27 000 ans pour un utilisateur moyen faisant 1 000 divisions par jour est contestable. D'une part, un utilisateur de tableur de logiciel scientifique ou de comptabilité fait beaucoup plus de 1 000 divisions par jour ; d'autre part, le taux d'erreurs du *Pentium* est dix millions de fois supérieur à la norme admise dans le monde des processeurs. Les ingénieurs d'*Intel* avaient commis une bourde dans la partie de la puce servant à faire les divisions, et cette erreur, gravée au plus profond de cinq millions de puces disséminées dans le monde entier, était vraiment ennuyeuse, quoi que prétende *Intel*.

Un analyste financier trouva des cas où le quatrième chiffre d'un résultat était faux. Un expert médical affirma que : «Toute erreur un tant soit peu significative dans une analyse de résultats est susceptible d'entraîner des conséquences sur la vie et la mort.» Pendant plusieurs mois, *Intel* fut l'objet de moqueries qui circulaient sur le réseau : «Combien de concepteurs du *Pentium* faut-il pour visser une ampoule ? Réponse : 1,999904274, mais c'est une bonne approximation pour un non technicien» ; «Pourquoi *Intel* a-t-il préféré le terme *Pentium* plutôt que 586, qui venait naturellement après le processeur 486? Parce qu'il a additionné 486 avec 100 en utilisant le *Pentium* et qu'il a trouvé 585,999990132», etc.

Les puces vendues aujourd'hui sont bien sûr exemptes du défaut qu'*Intel* a appris à repérer avant d'en vendre des millions : si votre machine est récente, vous n'avez rien à craindre.

L'ARITHMÉTIQUE JUSTIFIÉE ?

La découverte d'une telle erreur lors d'un calcul sur les nombres premiers a été saluée par de nombreux mathématiciens comme une preuve de leur propre utilité : il n'est pas absurde de mener de longs calculs arithmétiques qui poussent dans leurs retranchements les différents composants matériels et logiciels d'une machine, du processeur jusqu'au compilateur, et permettent de découvrir des erreurs qui, sinon, passeraient inaperçues.

Je ne pense pas que cela soit très sérieux. Il serait triste que les mathématiciens ne puissent justifier leur existence que par de tels exploits. On devrait affirmer que : «Les microprocesseurs sont utiles, car ils servent à faire de bonnes mathématiques», plutôt que l'inverse : «Les mathématiques sont utiles, car elles servent à faire de bons microprocesseurs.»

C'est la tentative, quelque peu scandaleuse, d'*Intel* de cacher ce qu'il savait qui a été dévoilée, et elle ne l'a été que parce que T. Nicely n'a pas renoncé à identifier la cause d'erreur. C'est finalement l'existence du monde universitaire, avec sa liberté, son esprit de curiosité et son exigence de rigueur poussée parfois jusqu'à l'absurde qui fut à l'origine de la découverte du camouflage. Une entreprise industrielle ou commerciale aurait-elle accepté qu'un de ses employés découvrant un problème – plutôt bénin – dans un programme mène la recherche de l'erreur plusieurs mois de suite jusqu'à la rechercher dans le microprocesseur ?

LES ÉCARTS ENTRE NOMBRES PREMIERS

L'objectif «premier» de T. Nicely était l'identification des records d'écarts entre nombres premiers. On sait que deux nombres premiers consécutifs peuvent être très écartés l'un de l'autre. Beaucoup plus difficile est de savoir quand un écart donné se produit pour la première fois.

La première fois que l'écart 6 apparaît est après 23, car 24, 25, 26, 27 et 28 sont composés (pour mesurer un écart, on considère la différence entre les deux nombres premiers qui encadrent les nombres composés consécutifs, 23 et 29 dans notre exemple). La première fois qu'apparaît l'écart 110 est après 370261. Aujourd'hui, grâce au programme de T. Nicely, on sait que la première fois que l'écart 906 apparaît, c'est après 218209405436543, et 906 est le plus grand nombre pour lequel on connaisse cette information.

Dans son article à paraître, T. Nicely remercie *Intel* pour un don d'ordinateur et pour l'aide apportée par plusieurs ingénieurs d'*Intel* dans le perfectionnement de son programme. Sans rancune !

D. Shanks a conjecturé que la taille de la première apparition de l'écart E se produit au nombre premier $p(E) \approx \exp \sqrt{E}$. Cette conjecture a été affinée par Weintraub qui proposa après expérimentation : $p(E) \approx \exp(\sqrt{1{,}165746\ E})$. Un argument heuristique proposé par Marek Wolf conduit à une conjecture plus fine encore : $p(E) \approx E^{1/2} \cdot \exp((\log^2(E) + 4E)^{1/2}/2)$

Les calculs de M. Wolf et de T. Nicely confirment cette loi. Il n'est pas étonnant ici que ce soit un physicien qui propose la conjecture la plus avancée, car, comme on ne sait quasi rien démontrer sur les écarts entre nombres premiers, l'arithmétique est sur ce point une science observationnelle proche de la physique, où l'on utilise des lois (bien sûr, non démontrées) pour en proposer d'autres (non démontrées) qu'éventuellement on pourra confirmer ou invalider par un calcul.

UN RÉSULTAT NOUVEAU ET TRÈS SIMPLE

Signalons une magnifique découverte récente concernant les écarts entre nombres premiers, due encore à M. Wolf, cette fois associé à A. Odlyzko et M. Rubinstein. Pour la tranche des nombres premiers qu'on explore systématiquement (aujourd'hui de 1 à environ 10^{15}), on constate que 6 est l'écart entre nombres premiers le plus fréquent. Doit-on alors penser qu'il en est toujours ainsi ?

Non, l'analyse heuristique et le calcul pour confirmation conduisent à penser qu'il y a changement du «champion» vers $1{,}7\ 10^{36}$, l'écart gagnant 6 étant alors remplacé par 30. Plus loin vers $5{,}81\ 10^{428}$, le champion devient 2 310, puis vers $1{,}48\ 10^{8656}$ il devient 30 030. La règle semble être que les champions successifs sont les produits des nombres premiers :
$6 = 2 \times 3$; $30 = 2 \times 3 \times 5$; $2\,310 = 2 \times 3 \times 5 \times 7$; $30\,030 = 2 \times 3 \times 5 \times 7 \times 11$; etc.

La conjecture affirmant que les choses sont réellement ainsi (c'est-à-dire qu'indéfiniment il y a changement des champions, qui sont successivement tous les produits de nombres premiers) est tellement éloignée de tout ce qu'on sait démontrer qu'on peut affirmer sans risque qu'avec l'étude de l'écart entre nombres premiers les mathématiciens ont de quoi s'occuper quelques siècles... si ce n'est un millénaire entier.

Jean-Paul DELAHAYE est professeur à l'Université de Lille. Adresse internet : delahaye@lifl.fr

C. CALDWELL, *The Prime Pages*. http://www.utm.edu/research/primes/

T. FORBES, *Prime k-tuplets*. http://www.ltkz.demon.co.uk/ktuplets.htm

J. M. MULLER, *Algorithmes de division pour microprocesseurs : illustration à l'aide du «Bug» du* Pentium, *Technique et science informatiques*, 14-8, pp. 1031-1049, 1985.

T. NICELY, Pentium *Division Flaw* : http/www.lynchburg.edu/public/academic/math/nicely/pentbug/pentbug.htm

T. NICEL, *Enumeration to 1e14 of the Twin Primes and Brun Constant*, in *Virginia Journal Science*, 46-3, pp. 195-204, 1996. http/www.lynchburg.edu/public/academic/math/nicely/twins/twins.htm

T. NICELY, *New Maximal Prime Gaps and First Occurences, Mathematics of Computation*, 1999 (article à paraître). http/www.lynchburg.edu/public/academic/math/nicely/gaps/gaps.htm