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 : $p(E) \approx E^{1/2}.\ \exp((\log^2(E) + 4E)^{1/2}/2)$

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