Premiers jumeaux : frères ennemis ?

JEAN-PAUL DELAHAYE

En additionnant les inverses des nombres premiers jumeaux, un mathématicien obstiné découvre des erreurs dans les microprocesseurs.

Il arrive que l'écart entre deux nombres premiers soit égal à 2. Ainsi le nombre premier 11 est suivi de 13, 17 de 19, 29 de 31, etc. Le problème, comme nous le verrons, est dans le etc.!

Ces paires sont dénommées des nombres premiers jumeaux ; si l'on ne sait pas très bien qui s'y intéressa le premier, elles sont l'objet d'une grande attention depuis un siècle. Leur étude a donné lieu à de nombreuses spéculations mathématiques et à de non moins nombreux calculs informatiques. L'un d'eux, dont les conclusions viennent d'être rendues disponibles, a mené un paisible mathématicien à faire trembler sur sa base la puissante industrie des microprocesseurs ; d'autres ont amené la découverte de nouvelles propriétés des nombres premiers. Ainsi, par certains côtés, l'arithmétique ressemble plus à une discipline expérimentale, proche de la physique, qu'à une branche des mathématiques dites «pures».

Thomas Nicely

1. LE BUG DU *PENTIUM* : AVEC THOMAS NICELY, TESTEZ VOTRE MACHINE!

Le problème du *Pentium*, dévoilé par Thomas Nicely, a été décortiqué, et des cas d'erreurs très simples ont été repérés. Le pire cas a été découvert par Tim Coe: 4195835.0 / 3145727.0 donne 1.333739068902... au lieu de 1.333820449136... sur le *Pentium*. L'erreur est 10 000 fois supérieure à celle que donne une calculette à 50 francs : il ne s'agit pas d'une erreur normale d'arrondi.

Pour le petit programme de trois instructions : $B = 4.1 - 1.1$; $A = 699306 * B$; $Q = A / B$, le *Pentium* donne $Q = 699263.3$ au lieu de $Q = 699306$. Dans ce programme, il ne faut pas remplacer 4.1 – 1.1 par 3, car le *Pentium* calcule en binaire et ni 4.1 ni 1.1 ne s'écrivent exactement en base 2.

Pour le quotient 4.9999999/14.999999 le *Pentium* donne 0.33332922 au lieu de 0.33333329. Là non plus, il ne s'agit pas d'une erreur normale d'arrondi, mais d'une erreur dans la conception même de l'algorithme de division du processeur mathématique des premières versions du *Pentium*.

Une analyse détaillée montre que c'est souvent avec des nombres proches de l'unité que le *Pentium* se trompe. Or il se trouve que, dans toutes sortes de calculs, de tels nombres apparaissent naturellement, ce qui fait que, même si peu de divisions sont mal calculées, ce sont par malchance des divisions qu'on a la plus grande probabilité de rencontrer. Vaughan Pratt a ainsi montré que, si l'on s'intéresse aux quotients x/y, avec x et y variant entre 1 et 100 par pas de 1/100000, la probabilité de tomber sur une erreur du *Pentium* est de 1/3000, ce qui est très loin du $1/9 \times 10^9$ indiqué par *Intel* pour se défendre!

L'erreur du *Pentium* n'est pas bénigne! Remarquons cependant que les erreurs d'arrondi sont normales et inévitables, et qu'elles se produisent même avec des microprocesseurs sans bug. Leur accumulation doit être contrôlée : un rapport du *General Accounting Office* américain cite le cas d'un missile *Patriot* qui, pendant la guerre du Golfe, n'a pas intercepté sa cible, à la suite d'accumulations d'erreurs d'arrondi, causant la mort de 28 personnes.

EN TROUVE-T-ON TOUJOURS ?

Existe-t-il une infinité de nombres premiers jumeaux? C'est l'une des plus célèbres conjectures mathématiques : on ne sait ni prouver qu'il n'y a qu'un nombre fini de nombres premiers jumeaux ni démontrer le contraire. La situation est choquante, car moins de 30 mots suffisent pour démontrer qu'il existe une infinité de nombres premiers : *S'il n'y en avait qu'un nombre fini, leur produit additionné de 1 serait divisible par l'un d'eux, donc 1 aussi, ce qui est absurde*. En même temps, tout semble s'opposer à ce que l'on sache (avec certitude) si, oui ou non, il existe une infinité de nombres premiers jumeaux. Les deux problèmes sont très proches, pourtant l'un est facile, alors que l'autre résiste obstinément.

Bien sûr, les calculs montrent que l'on trouve toujours des nombres premiers jumeaux, aussi loin qu'on aille. On a cherché aussi à compter le nombre précis de premiers jumeaux inférieurs à n. Ce calcul, par recherche exhaustive, a été mené jusqu'à la valeur de n égale à 10^{15} (un million de milliards) : pour 29 844 570 422 669 nombres premiers inférieurs à 10^{15}, on compte exactement 1 177 209 242 304 paires de nombres premiers jumeaux, soit environ quatre pour cent.

Les mathématiciens ont trouvé des nombres jumeaux beaucoup plus grands que cette valeur. Actuellement, la plus grande paire, découverte il y a quelques semaines, est composée de deux nombres de 11 755 chiffres chacun, qui sont : 361700055.2^{39014} plus et moins 1. Ces nombres ont été capturés par Henri Lifchitz, un ingénieur français passionné des nombres premiers (en 1971, il avait déjà publié une table des nombres premiers inférieurs à 20 millions).

Les nombres premiers se raréfient ;

aux alentours de n, il y a environ $1/\log n$ nombres premiers (exemple : puisque $\log 1\,000\,000$ égale 13,81, vers le millionième nombre entier, il y a environ un nombre premier sur 14). Ce «théorème des nombres premiers» a été démontré en même temps par le Français Jacques Hadamard et le Belge Charles-Jean de la Vallée Poussin en 1896. (Ils vécurent respectivement jusqu'à l'âge de 98 et 96 ans : le meilleur moyen pour vivre âgé est de démontrer un tel théorème !)

Raréfaction

On constate que les nombres premiers jumeaux considérés parmi les nombres premiers se raréfient aussi. Un argument heuristique (c'est-à-dire qui «suggère» sans prouver rigoureusement) conduit à penser que les nombres premiers jumeaux ont une densité égale à $1/\log n$ parmi les nombres premiers (ou, ce qui revient au même, une densité de $1/(\log n)^2$ parmi les nombres entiers). L'argument est simple : «la probabilité que p et que $p + 2$ soient simultanément premiers est le produit de la probabilité que p soit premier par celle que $p + 2$ le soit, car les événements sont indépendants et "donc" le "$1/\log n$" du théorème des nombres premiers fournit un "$1/(\log n)^2$" (car la probabilité de la conjonction de deux événements indépendants est le produit de leurs probabilités).

Cet argument est non seulement insuffisant, mais extrêmement dangereux. En l'appliquant à p et à p +1, on déduit que la densité des paires de nombres consécutifs premiers est $1/(\log n)^2$, alors qu'elle est nulle, puisque, quel que soit p, l'un des deux nombres p ou p +1 est pair.

G. Hardy et J. Littlewood ont proposé une conjecture (toujours non prouvée, bien sûr) selon laquelle le nombre noté $\pi_2(m)$ de nombres premiers jumeaux inférieurs à m est approché par la formule : $\pi_2(m) \approx 2\, C_j\, m / (\log m)^2$, où C_j est la constante des nombres premiers jumeaux. Dans la formule définissant C_j, les nombres p sont premiers :
$C_j = (1–1/2^2)(1–1/4^2)(1–1/6^2)...(1–1/(p–1)^2)...$
$= 0{,}660161815846869573927812 1...$

On pourrait être tenté de rire du culot des mathématiciens : incapables de montrer qu'il y a une infinité de nombres premiers jumeaux, ils énoncent des résultats considérablement plus forts (donc plus difficiles) concernant leur répartition ! Leur attitude est celle d'un alpiniste qui, après avoir échoué dans l'ascension du Mont-Blanc, annoncerait : «Ça ne fait rien, ma prochaine escalade sera l'Everest.» Ce culot est cependant justifié : en mathématiques, il est souvent arrivé qu'on aboutisse dans une recherche en prouvant un théorème beaucoup plus général et plus fort que celui que l'on visait initiale-

2. LES NOMBRES PREMIERS JUMEAUX

(a) Nombres premiers et premiers jumeaux jusqu'à 2000

Les nombres premiers jumeaux sont séparés de deux unités. La conjecture des nombres premiers jumeaux affirme qu'il y en a une infinité. On a proposé une conjecture précise : il y en aurait environ $1{,}32\, n /(\log n)^2$ parmi les nombres inférieurs à n.

2	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59	
61	67	71	73	79	83	89	97	101	103	107	109	113	127	131	137	139	
149	151	157	163	167	173	179	181	191	193	197	199	211	223	227	229	233	
239	241	251	257	263	269	271	277	281	283	293	307	311	313	317	331	337	
347	349	353	359	367	373	379	383	389	397	401	409	419	421	431	433	439	
443	449	457	461	463	467	479	487	491	499	503	509	521	523	541	547	557	
563	569	571	577	587	593	599	601	607	613	617	619	631	641	643	647	653	
659	661	673	677	683	691	701	709	719	727	733	739	743	751	757	761	769	
773	787	797	809	811	821	823	827	829	839	853	857	859	863	877	881	883	
887	907	911	919	929	937	941	947	953	967	971	977	983	991	997	1009	1013	
1019	1021	1031	1033	1039	1049	1051	1061	1063	1069	1087	1091	1093	1097	1103	1109	1117	
1123	1129	1151	1153	1163	1171	1181	1187	1193	1201	1213	1217	1223	1229	1231	1237	1249	
1259	1277	1279	1283	1289	1291	1297	1301	1303	1307	1319	1321	1327	1361	1367	1373	1381	
1399	1409	1423	1427	1429	1433	1439	1447	1451	1453	1459	1471	1481	1483	1487	1489	1493	
1499	1511	1523	1531	1543	1549	1553	1559	1567	1571	1579	1583	1597	1601	1607	1609	1613	
1619	1621	1627	1637	1657	1663	1667	1669	1693	1697	1699	1709	1721	1723	1733	1741	1747	
1753	1759	1777	1783	1787	1789	1801	1811	1823	1831	1847	1861	1867	1871	1873	1877	1879	
1889	1901	1907	1913	1931	1933	1949	1951	1973	1979	1987	1993	1997	1999	2003			

(b) Raréfaction des nombres premiers jumeaux

	nombres de nombres premiers	*nombres de premiers jumeaux*	*pourcentages de premiers jumeaux*
10^3	168	35	20,83
10^4	1229	205	16,68
10^5	9592	1224	12,76
10^6	78498	8169	10,41
10^7	664579	58980	8,87
10^8	5761455	440312	7,65
10^9	50847534	3424506	6,73
10^{10}	455052511	27412679	6,02
10^{11}	4118054813	224376048	5,45
10^{12}	37607912018	1870585220	4,97
10^{13}	346065536839	15834664872	4,56
10^{14}	3204941750802	135780321665	4,22
10^{15}	29844570422669	1177209242304	3,94

(c) Les plus grandes paires de premiers jumeaux connues

$835335 \times 2^{39014} \pm 1$	11751 chiffres	Ballinger et Gallot 1998
$242206083 \times 2^{3880} \pm 1$	11713 chiffres	Jarai et Indlekofer 1995
$40883037 \times 2^{3356} \pm 1$	6696 chiffres	Lifchitz et Gallot 1998
$361700055 \times 2^{39020} \pm 1$	11755 chiffres	Lifchitz 1999

(d) Caractérisations et formules

n est le premier élément d'une paire de nombres premiers jumeaux si et seulement si :
$4((n–1)! +1) + n$ est un multiple de $n(n+2)$
ou $(n–1)!(3n+2)+2n+2$ est un multiple de $n(n+2)$
ou $(n–1)!(n–2)–2$ est un multiple de $n(n+2)$.
On en déduit que la formule suivante engendre tous les nombres premiers jumeaux quand n décrit l'ensemble des entiers ≥ 0 :
$j(n) = 3+n[(4(n+2)!+n+7)/(n+3)(n+5)–[(4(n\ 2)!+n\ 6)/(n+3)(n+5)]]$.

(e) Polynôme qui donne tous les nombres premiers jumeaux

Lorsque les variables $a, b, ..., z$ décrivent l'ensemble des entiers positif ou nul, les valeurs positives du polynôme suivant, dû à Christoph Baxa (et tiré de la théorie des équations diophantiennes), décrivent l'ensemble des nombres p tels que p, $p + 2$ constituent une paire de premiers jumeaux :
$(k+2)(1–(wz+h+j-q)^2–((g+1)(h+j)+h–z)^2–(p+q+z+2n–e)^2$
$–(e^3(e+2)(a+1)^2+1–o^2)^2–((a^2–1)(n+l+v)^2+1–x^2)^2–(16(a^2–1)(n+l+v)^2+1–x^2)^2$
$–(((a+u^2(u^2–a))^2–1)(n+4d(n+l+v))^2+1–(x+cu)^2)^2–((a^2–1)l^2+1–m^2)^2$
$–(p+l(a–n–1)+b(2a(n+1)–(n+1)2–1)–m)^2–(q+(n+l+v)(a–p–1)$
$+s(2a(p+1)–(p+1)^2–1)–x)^2–(z+pl(a–p)+t(2ap–p^2–1)–pm)^2$
$–(16(k+1)3(k+2)(n+1)2+1–f^2)^2–(k+1+ia–i–l)^2–(4g+k+10–y(k+2)(k+4))^2)$.

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 :

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

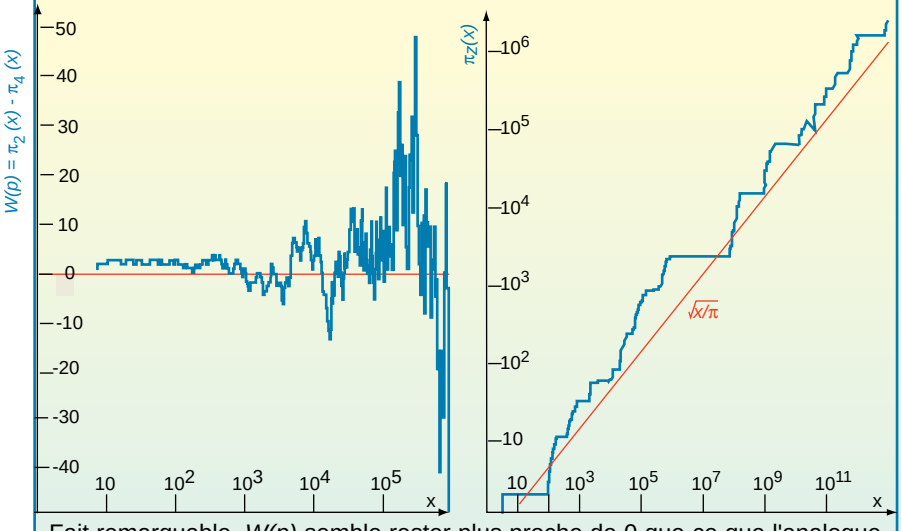
avec C_j = 0,6601618158468... constante des nombres premiers jumeaux

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

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.

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