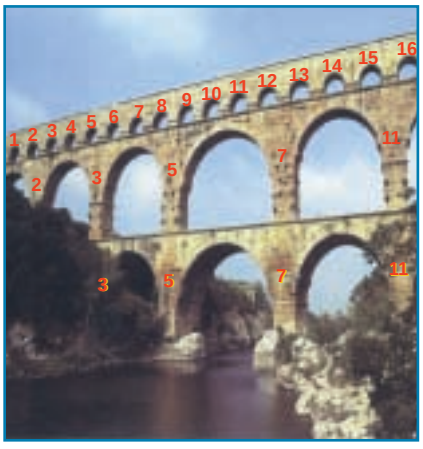

Premiers jumeaux : frères ennemis?

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 :

$$(k+2)(1–(wz+h+j-q)^2–((g+1)(h+j)+h–z)^2–(p+q+z+2n–e)^2$$
$$–(e^3(e+2)(a+1)^2+1–o^2)^2–((a^2–1)(n+l+v)^2+1–x^2)^2–(16(a^2–1)(n+l+v)^2+1–x^2)^2$$
$$–(((a+u^2(u^2–a))^2–1)(n+4d(n+l+v))^2+1–(x+cu)^2)^2–((a^2–1)l^2+1–m^2)^2$$
$$–(p+l(a–n–1)+b(2a(n+1)–(n+1)2–1)–m)^2–(q+(n+l+v)(a–p–1)$$
$$+s(2a(p+1)–(p+1)^2–1)–x)^2–(z+pl(a–p)+t(2ap–p^2–1)–pm)^2$$
$$–(16(k+1)3(k+2)(n+1)2+1–f^2)^2–(k+1+ia–i–l)^2–(4g+k+10–y(k+2)(k+4))^2).$$