



Un nombre premier à 50 000 \$

JEAN-PAUL DELAHAYE

En utilisant des milliers d'ordinateurs oisifs, vous avez gratuitement une énorme puissance de calcul.

Nayan Hajratwala, de Plymouth (Michigan), vient de prouver avec son ordinateur personnel que $2^{8972593} - 1$ est un nombre premier (c'est-à-dire n'est divisible que par un et par lui-même). C'est le plus grand nombre premier connu, et nous sommes sûr du résultat, car la preuve a été refaite sur un autre ordinateur indépendant.

Le nombre $2^{8972593} - 1$ est un nombre premier de Mersenne, c'est-à-dire de la forme $2^p - 1$. Ces nombres intéressent les mathématiciens depuis longtemps, et celui-ci est le 38^e nombre premier de Mersenne. Il a 2 098 960 chiffres : l'écrire

occuperait, en petits caractères, un numéro complet de *Pour la Science*. Il permet à N. Hajratwala de remporter les 50 000 \$ du prix créé il y a quelques mois pour récompenser la première personne ou équipe proposant un nombre premier de plus de un million de chiffres.

L'ordinateur utilisé pour prouver que ce nombre est premier est un micro-ordinateur banal comme vous en possédez peut-être un. C'est un IBM-Aptiva équipé d'un processeur Pentium II fonctionnant à la vitesse d'horloge de 350 Mhz. L'ordinateur a calculé pendant 111 jours (trois semaines auraient suffi s'il avait calculé

sans s'arrêter). Le calcul n'a pas dérangé son propriétaire, car le programme ne fonctionnait que pendant les périodes où N. Hajratwala laissait sa machine inoccupée (mais branchée!).

N. Hajratwala n'est pas un mathématicien de génie, et il n'est même pas certain qu'il sache précisément ce que fait le programme qui lui a permis de gagner et qu'il a téléchargé sur le site Internet du projet GIMPS : *Great Internet Mersenne Prime Search*.

LA LOTERIE DU CALCUL

Le projet GIMPS a été fondé en janvier 1996 par George Woltman, un informaticien à la retraite qui vit à Orlando, en Floride. Il concentre et organise la puissance de calcul gisant inexploitée dans les milliers d'ordinateurs personnels répartis dans le monde pour améliorer notre connaissance des nombres premiers.

N. Hajratwala a eu de la chance, car il n'était pas le seul à essayer de trouver un nombre premier de plus de un million de chiffres. Les organisateurs du projet GIMPS ont confié des calculs à plus de 21 000 ordinateurs. Chaque participant essayait son propre nombre de Mersenne, lequel, le plus souvent, n'est pas premier : aussi n'avait-il qu'une chance sur 30 000 environ de tomber sur un nombre premier. Ainsi, participer au projet GIMPS avec sa machine revenait à jouer à la loterie : contre le prix de l'électricité nécessaire au fonctionnement de la machine et l'usure que le calcul ininterrompu peut provoquer (tout cela constituant l'équivalent du coût du billet de loterie), vous aviez droit à un exposant (l'équivalent d'un numéro de loterie) qui vous permettait d'espérer le prix.

Le prochain prix sera donné pour un nombre premier de dix millions de chiffres, mais les organisateurs souhaitent d'abord explorer tous les exposants n assez petits pour connaître parfaitement et définitivement quels sont, parmi les nombres

1. MARIN MERSENNE (OIZÉ 1588 - PARIS 1648)

Après des études chez les oratoriens du Mans, puis chez les jésuites à La Flèche, il prend l'habit des minimes (ordre qui doit son nom au désir que les moines avaient d'être les plus humbles des serviteurs de Dieu). Il enseigne la philosophie à Nevers, puis s'établit à Paris. Il publie divers ouvrages de sciences et de philosophie, dont, en 1624, un livre au titre charmant : *L'impiepiété des déistes, athées et libertins, renversée et confondue*. Il défend la théorie de Galilée contre les critiques des théologiens et s'oppose à l'alchimie et à l'astrologie qu'il dénonce comme pseudo-sciences. Le père Mersenne



entretient une correspondance avec les plus grands savants de son époque : Descartes, Pascal, Torricelli, Gassendi, Hobbes, Huygens, Roberval. Après sa mort, on trouvera dans ses affaires des lettres de 78 savants différents. Il rend visite à Fermat à Toulouse et c'est le premier physicien à utiliser le pendule pour mesurer l'intensité de la pesanteur. Il conçoit un hygromètre et un télescope à miroir parabolique, il découvre la loi des tuyaux sonores et des cordes vibrantes, ce qui lui permet de comprendre le rapport entre la hauteur des notes de la gamme musicale et la fréquence, il mesure aussi la vitesse du son.

Mersenne affirme en 1644 que $M_p = 2^p - 1$ est un nombre premier pour p égal à 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257, et composé, pour les autres exposants, jusqu'à 257. Persuvin et Seelhoff relèvent, en 1886, une première erreur dans la liste de Mersenne : ils prouvent que M_{61} est premier. Quatre autres erreurs sont découvertes par la suite : M_{67} et M_{257} ne sont pas premiers, alors que M_{89} et M_{107} le sont.

On ignore encore si, parmi les nombres de la forme $M_p = 2^p - 1$ avec p premier (les nombres de Mersenne), il y en a une infinité de premiers. On ignore aussi s'il y a une infinité de nombres de Mersenne composés. Bien sûr, l'une au moins des affirmations est vraie, probablement les deux.

de la forme $2^n - 1$, ceux qui sont premiers. Ils souhaitent savoir si le nombre trouvé par N. Hajratwala n'est pas précédé par d'autres nombres de Mersenne premiers.

La puissance de calcul obtenue par le système de répartition des tâches de GIMPS via l'Internet est impressionnante. On l'évalue à 700 milliards d'opérations en virgule flottante par seconde, soit l'équivalent des plus puissants ordinateurs vectoriels actuels, tel le CRAY T932.

Les machines utilisées aujourd'hui pour la prévision météorologique et le calcul scientifique coûtent des fortunes, et il est hors de question de les faire travailler à la recherche de nombres premiers pendant des mois d'affilée! Sans le calcul réparti, ce calcul de nombres

de Mersenne n'aurait sans doute pas abouti avant une dizaine d'années.

Si les organisateurs du projet GIMPS devaient acheter leurs calculs auprès de grands centres informatiques, cela leur coûterait environ 200 000 \$ par jour. Il est heureux que ce calcul ait été gratuit, sinon les organisateurs auraient dépensé plus que les 50 000 \$ du prix.

Certains algorithmes au cœur du programme que chaque participant au projet GIMPS installe sur sa machine et fait fonctionner quand il ne s'en sert pas sont assez anciens, d'autres ont été récemment perfectionnés. On évalue qu'avec les algorithmes actuels le prochain prix (pour un nombre premier de dix millions de chiffres) demandera 125 fois plus de calculs. On disposera de cette ressource de calculs grâce à la puissance accrue

des prochains microprocesseurs et par l'augmentation de leur nombre. Si l'on attend les progrès des microprocesseurs, il faudra sept doublements de puissance, soit, à raison d'un doublement tous les 18 mois (loi de Moore), environ dix ans. Si l'on incitait tous les possesseurs de micro-ordinateurs de la Terre à participer au projet, alors l'affaire pourrait être réglée en quelques semaines. Le prochain prix tombera, par une combinaison des deux méthodes, dans trois à quatre ans.

LES NOMBRES PARFAITS

À chaque nombre premier de Mersenne correspond un nombre parfait, un nombre égal à la somme de ses diviseurs (autres que lui-même) : au nombre premier de Mersenne $2^n - 1$ correspond le nombre

2. LES NOMBRES PREMIERS DE MERSENNE				3. NOMBRES PREMIERS RECORDS				
Les nombres premiers $M_p = 2^p - 1$, dénommés nombres premiers de Mersenne, connus aujourd'hui sont :				Le plus grand nombre premier obtenu avec et sans ordinateurs (d'après C. Caldwell)				
n	p	année du calcul	auteur du calcul	nombre de chiffres	nombre	année	auteur	méthode
1	2			$2^{17} - 1$	6	1588?	Cataldi	Division
2	3			$2^{19} - 1$	6	1588?	Cataldi	Division
3	5			$2^{31} - 1$	10	1772?	Euler	Division et raisonnement
4	7			$(2^{59} - 1)/179951$	13	1867	Landry	Division et raisonnement
5	13	1588	P. Cataldi	$2^{127} - 1$	39	1876	Lucas	Suite de Lucas
6	17	1588	P. Cataldi	$(2^{148} + 1)/17$	44	1951	Ferrier	Théorème de Proth
7	19	1750	L. Euler					
8	31	1883	I. Pervushin					
9	61	1911	R. Powers					
10	89	1913	E. Fauquembergue					
11	107	1876	E. Lucas					
12	127	1952	R. Robinson	$180(M_{127})^2 + 1$	79	1951	EDSAC1	Miller & Wheeler
13	521	1952	R. Robinson	M_{521}	157	1952	SWAC	Robinson (30 janv.)
14	607	1952	R. Robinson	M_{607}	183	1952	SWAC	Robinson (30 janv.)
15	1279	1952	R. Robinson	M_{1279}	386	1952	SWAC	Robinson (25 juin)
16	2203	1952	R. Robinson	M_{2203}	664	1952	SWAC	Robinson (7 oct.)
17	2281	1952	R. Robinson	M_{2281}	687	1952	SWAC	Robinson (9 oct.)
18	3217	1957	H. Riesel	M_{3217}	969	1957	BESK	Riesel
19	4253	1961	A. Hurwitz	M_{4253}	1281	1961	IBM7090	Hurwitz
20	4423	1961	A. Hurwitz	M_{4423}	1332	1961	IBM7090	Hurwitz
21	9689	1963	D. Gillies	M_{9689}	2917	1963	ILLIAC 2	Gillies
22	9941	1963	D. Gillies	M_{9941}	2993	1963	ILLIAC 2	Gillies
23	11213	1963	D. Gillies	M_{11213}	3376	1963	ILLIAC 2	Gillies
24	19937	1971	B. Tuckerman	M_{19937}	6002	1971	IBM360/91	Tuckerman
25	21701	1978	L. Noll et L. Nickel	M_{21701}	6533	1978	Cyber 174	Noll et Nickel
26	23209	1979	L. Noll	M_{23209}	6987	1979	Cyber 174	Noll
27	44497	1979	H. Nelson et D. Slowinski	M_{44497}	13395	1979	Cray 1	Nelson et Slowinski
28	86243	1982	D. Slowinski	M_{86243}	25962	1982	Cray 1	Slowinski
29	110503	1988	W. Colquitt et L. Welsh	M_{132049}	39751	1983	Cray X-MP	Slowinski
30	132049	1983	D. Slowinski	M_{216091}	65050	1985	Cray X-MP	Slowinski
31	216091	1988	D. Slowinski	$391581 \cdot 2^{216193} - 1$	65087	1989	Amdahl	Brown et al
32	756839	1992	D. Slowinski	M_{756839}	227832	1992	Cray-2	Slowinski et Gage
33	859433	1994	D. Slowinski et Gage	M_{859433}	258716	1994	Cray C90	Slowinski et Gage
34	1257787	1996	D. Slowinski et Gage	$M_{1257787}$	378632	1996	Cray T94	Slowinski et Gage
35	1398269	1996	Woltman, Armengaud (GIMPS)	$M_{1398269}$	420921	1996	Pentium	GIMPS
36	2976221	1997	Woltman, Spence (GIMPS)	$M_{2976221}$	895932	1997	Pentium	GIMPS
37	3021377	1998	Woltman et al. (GIMPS)	$M_{3021377}$	909526	1998	Pentium	GIMPS
38	8972593	1999	Woltman et al. (GIMPS)	$M_{8972593}$	2098960	1999	Pentium II	GIMPS