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

Les nombres premiers $M_p = 2^p - 1$, dénommés nombres premiers de Mersenne, connus aujourd'hui sont :

n	p	année du calcul	auteur du calcul
1	2		
2	3		
3	5		
4	7		
5	13		
6	17	1588	P. Cataldi
7	19	1588	P. Cataldi
8	31	1750	L. Euler
9	61	1883	I. Pervushin
10	89	1911	R. Powers
11	107	1913	E. Fauquembergue
12	127	1876	E. Lucas
13	521	1952	R. Robinson
14	607	1952	R. Robinson
15	1279	1952	R. Robinson
16	2203	1952	R. Robinson
17	2281	1952	R. Robinson
18	3217	1957	H. Riesel
19	4253	1961	A. Hurwitz
20	4423	1961	A. Hurwitz
21	9689	1963	D. Gillies
22	9941	1963	D. Gillies
23	11213	1963	D. Gillies
24	19937	1971	B. Tuckerman
25	21701	1978	L. Noll et L. Nickel
26	23209	1979	L. Noll
27	44497	1979	H. Nelson et D. Slowinski
28	86243	1982	D. Slowinski
29	110503	1988	W. Colquitt et L. Welsh
30	132049	1983	D. Slowinski
31	216091	1988	D. Slowinski
32	756839	1992	D. Slowinski
33	859433	1994	D. Slowinski et Gage
34	1257787	1996	D. Slowinski et Gage
35	1398269	1996	Woltman, Armengaud (GIMPS)
36	2976221	1997	Woltman, Spence (GIMPS)
37	3021377	1998	Woltman et al. (GIMPS)
38	8972593	1999	Woltman et al. (GIMPS)

3. NOMBRES PREMIERS RECORDS

Le plus grand nombre premier obtenu avec et sans ordinateurs (d'après C. Caldwell)

nombre	nombre de chiffres	année	auteur	méthode
$2^{17} - 1$	6	1588?	Cataldi	Division
$2^{19} - 1$	6	1588?	Cataldi	Division
$2^{31} - 1$	10	1772?	Euler	Division et raisonnement
$(2^{59} - 1)/179951$	13	1867	Landry	Division et raisonnement
$2^{127} - 1$	39	1876	Lucas	Suite de Lucas
$(2^{148} + 1)/17$	44	1951	Ferrier	Théorème de Proth

		ordinateurs	auteur ou équipe
$180(M_{127})^2+1$	79	1951	EDSAC1	Miller & Wheeler
M_{521}	157	1952	SWAC	Robinson (30 janv.)
M_{607}	183	1952	SWAC	Robinson (30 janv.)
M_{1279}	386	1952	SWAC	Robinson (25 juin)
M_{2203}	664	1952	SWAC	Robinson (7 oct.)
M_{2281}	687	1952	SWAC	Robinson (9 oct.)
M_{3217}	969	1957	BESK	Riesel
M_{4253}	1281	1961	IBM7090	Hurwitz
M_{4423}	1332	1961	IBM7090	Hurwitz
M_{9689}	2917	1963	ILLIAC 2	Gillies
M_{9941}	2993	1963	ILLIAC 2	Gillies
M_{11213}	3376	1963	ILLIAC 2	Gillies
M_{19937}	6002	1971	IBM360/91	Tuckerman
M_{21701}	6533	1978	Cyber 174	Noll et Nickel
M_{23209}	6987	1979	Cyber 174	Noll
M_{44497}	13395	1979	Cray 1	Nelson et Slowinski
M_{86243}	25962	1982	Cray 1	Slowinski
M_{132049}	39751	1983	Cray X-MP	Slowinski
M_{216091}	65050	1985	Cray X-MP	Slowinski
$391581*2^{216193}-1$	65087	1989	Amdahl	Brown et al
M_{756839}	227832	1992	Cray-2	Slowinski et Gage
M_{859433}	258716	1994	Cray C90	Slowinski et Gage
$M_{1257787}$	378632	1996	Cray T94	Slowinski et Gage
$M_{1398269}$	420921	1996	Pentium	GIMPS
$M_{2976221}$	895932	1997	Pentium	GIMPS
$M_{3021377}$	909526	1998	Pentium	GIMPS
$M_{8972593}$	2098960	1999	Pentium II	GIMPS

4. POUR QUE M_p SOIT PREMIER, IL FAUT QUE p SOIT PREMIER

Pour qu'un nombre de la forme $2^p - 1 = M_p$ soit un nombre premier, il faut que p soit un nombre premier (cette condition n'est pas suffisante).
En effet, si p est composé, $p = a.b$ avec $a > 1$ $b > 1$, alors on utilise l'identité :
$X^n - 1 = (X - 1)(X^{n-1} + X^{n-2} + ... + X^2 + X + 1)$
qui, en prenant $X = 2^a$ et $n = b$, donne :
$2^p - 1 = 2^{ab} - 1 = (2^a)^b - 1 = (2^a - 1)((2^a)^{b-1} + (2^a)^{b-2} + ... + (2^a) + 1)$.
Si la condition était suffisante, on aurait une formule simple donnant une infinité de nombres premiers.

parfait $2^{n-1}(2^n - 1)$. On montre que, réciproquement, tout nombre parfait pair s'obtient à partir d'un nombre premier de Mersenne. Pour n égal à 2, $2^n - 1 = 3$ est premier et donc $2^{n-1}(2^n - 1) = 6$ est un nombre parfait pair ($6 = 1 + 2 + 3$). Pour n égal à 3, $2^n - 1 = 7$ est un nombre premier et $2^{n-1}(2^n - 1) = 28$ est un nombre parfait ($28 = 1 + 2 + 4 + 7 + 14$).

Le nombre parfait pair associé au nouveau nombre premier de Mersenne possède 4 197 919 chiffres. C'est bien sûr le plus grand nombre parfait connu. On ignore s'il existe une infinité de nombres parfaits pairs. Plus amusant, bien que le problème soit connu depuis plus de 2 500 ans, on ne sait pas s'il existe des nombres parfaits impairs. Personne n'en a jamais trouvé, personne n'a démontré qu'il n'en existait pas !

L'HISTOIRE DU PLUS GRAND NOMBRE PREMIER

Revenons sur l'histoire des nombres premiers records pour prendre conscience, en suivant ces records, comme ceux concernant les décimales de π, de l'explosion récente des connaissances mathématiques et techniques : pendant des siècles, tout a été très lent, puis, en quelques années, une série de résultats mathématiques et d'avancées techniques nous a fait formidablement progresser.

Avant le XVIe siècle, il est impossible de dresser la table précise des records du «plus grand nombre premier» : trop peu de documents nous sont parvenus, et il est impossible de valider une affirmation de primalité quand elle n'est pas accompagnée d'un minimum de justifications. S'il suffisait à un mathématicien de dire que tel nombre est premier pour que l'on considère que ledit mathématicien détient le record du plus grand nombre premier, alors, en affirmant que tous les nombres de Mersenne ($M_p = 2^p - 1$, avec p premier) sont premiers, on détiendrait le record jusqu'à la fin des temps : il est vraisemblable que, parmi ces nombres, il y en a une infinité de premiers et donc, même si l'on se trompe pour certains, on aura l'injuste gloire d'avoir proposé une primalité pour un nombre plus grand que ceux connus à un instant donné.

L'histoire du plus grand nombre premier commence donc à la fin du XVIe siècle. En 1588, Pietro Cataldi vérifie que $M_{17} = 2^{17} - 1 = 131\,071$ et $M_{19} = 2^{19} - 1 = 524\,287$ sont premiers. La table de nombres premiers qu'il a établie jusqu'à l'entier 750 suggère qu'il a bien fait les calculs nécessaires pour prouver la primalité de ces deux nombres en utilisant la méthode des divisions (on s'assure qu'aucune division de l'entier M par un nombre premier inférieur à la racine carrée de M ne tombe juste). Malheureusement, Cataldi indique aussi que $M_n = 2^n - 1$ est premier pour n = 23, 29, 31 et 37. Or c'est faux, sauf pour 31.

En 1640, Fermat, utilisant sa découverte que si p est impair et premier alors les diviseurs premiers de $2^p - 1$ sont de la forme $2kp + 1$, montre la fausseté des affirmations de Cataldi pour $n = 23$ et 37.

Euler montre plus tard encore que, pour 31, Cataldi avait raison et que, pour 29, il se trompait. Assez étrangement, les facteurs trouvés pour 23, 29 et 37 sont assez petits, et donc, si Cataldi avait utilisé sa table systématiquement, il aurait dû les découvrir. Cela rend suspectes ses affirmations pour 17 et 19.

La méthode d'Euler, qui prouve que Cataldi a raison pour $n = 31$, consiste à établir, dans un premier temps, que les diviseurs premiers de $2^{31} - 1 = 2147483647$ sont nécessairement de la forme $248n + 1$ ou $248n + 63$, puis, dans un second temps, à exploiter ce résultat en opérant une série judicieuse et limitée de divisions.

La leçon de l'histoire du plus grand nombre premier est que tout progrès résulte de l'amélioration des méthodes plutôt que de l'obstination de calculateurs fous, prêts à mener des suites d'opérations de plus en plus longues et pénibles.

Les derniers records où l'on fait calculer des réseaux de très nombreuses machines ne contredisent pas le principe que le record du plus grand nombre premier est le fruit de l'intelligence et de l'innovation. Si, dans les derniers calculs du projet GIMPS, la nouveauté n'est pas strictement mathématique, elle réside dans la maîtrise et dans l'application optimisée et organisée à grande échelle d'une technique nouvelle, où il n'est pas plus facile d'être le meilleur qu'en mathématiques.

Le record suivant de Landry en 1867 est obtenu avec $(2^{59} - 1)/179\,951 = 3\,203\,431\,780\,337$. Ce record doit être remarqué, car ce nombre premier n'est pas un nombre de Mersenne et c'est, parmi les nombres records qui ne sont pas des nombres de Mersenne, celui qui a tenu le plus longtemps : neuf ans.

En 1876, le Français Édouard Lucas propose une méthode plus efficace encore que celles de Fermat et d'Euler pour tester si un nombre de Mersenne est premier. Cette méthode, simplifiée par Lehmer dans les années 1930, est encore utilisée aujourd'hui pour les records de plus grands nombres premiers.

Le nombre prouvé premier par Lucas en 1876 est : $2^{127} - 1$ et il restera le plus grand nombre premier connu pendant 75 ans, jusqu'en 1951. C'est à cette date que Ferrier, à l'aide d'une machine à calculer mécanique de bureau, améliore le record de Lucas en découvrant un nombre premier de 44 chiffres : $(2^{148} + 1)/17$.

LES ORDINATEURS S'Y METTENT

Commence alors le temps des machines électroniques, dont la naissance dans les années 1940 permet d'aller plus loin grâce aux progrès technologiques (rapidité, fiabilité et puissance des circuits), à des innovations dans les algorithmes mathématiques de manipulation des grands nombres et à une meilleure maîtrise des langages de programmation.

En 1951, Miller et D. Wheeler prouvent, à l'aide de l'ordinateur EDSAC qui est moins puissant que nos calculatrices de poche d'aujourd'hui, puisqu'il dispose seulement d'une mémoire de 5 kilo-octets), que les nombres suivants sont premiers : $k\,M_{127} + 1$ pour k = 114, 124, 388, 408, 498, 696, 738, 744, 780, 934 et 978.

5. MÉTHODES POUR PROUVER LA PRIMALITÉ DES GRANDS NOMBRES

Le test de Lucas-Lehmer
$2^p - 1$ est un nombre premier si et seulement si $2^p - 1$ divise $S(p - 1)$
avec $S(1) = 4$ et $S(n + 1) = S(n)^2 - 2$ pour $n > 1$.

Le théorème de Proth (1878)
Si N est de la forme $N = k.2^n + 1$ avec $k < 2n$
et s'il existe un nombre entier a tel que : $a^{(N-1)/2} + 1 = 0 \pmod N$,
alors : N est premier.

Ces deux chercheurs découvrent aussi que le nombre de 79 chiffres suivant est premier : 180 $(M_{127})^2 + 1 = 180(2^{127} - 1)^2 + 1$. Ce nombre ne gardera le titre que peu de temps. L'année suivante, Raphaël Robinson écrit, pour l'ordinateur SWAC, son premier programme, qui marche du premier coup (!) et découvre, dans la journée du 30 janvier 1951, deux nouveaux nombres de Mersenne premiers (M_{521}, M_{607}). Les autres sont découverts le 25 juin (M_{1279}), le 7 octobre (M_{2203}) et le 9 octobre (M_{2281}).

En 1957, H. Riesel découvre que M_{3217} est premier à l'aide de l'ordinateur suédois BESK. De son côté, A. Hurwitz découvre que M_{4253} et M_{4423} sont premiers à l'aide d'un IBM7090. D. Gillies avec un ILLIAC-2 prouve la primalité de M_{9689}, M_{9941} et M_{11213}, et B. Tuckerman utilisant le célèbre IBM 360 met à jour le nombre premier M_{19937} qui comporte 6 002 chiffres.

Le calcul de Hurwitz pose un problème philosophique étrange. Hurwitz, à cause de l'ordre dans lequel la machine faisait apparaître les résultats, prit connaissance de la primalité de M_{4423} quelques secondes avant de lire que M_{4253} est aussi premier. Seul l'ordinateur IBM 7090 a cru que M_{4253} était premier avant d'afficher que M_{4423} était premier. Peut-on considérer que M_{4253} est un nombre premier record et faut-il l'indiquer dans les tables?

J'ai choisi de faire apparaître M_{4253} dans la table des records de nombres premiers les plus longs. Cela revient à attribuer la découverte à l'ordinateur lui-même, ce qui choquera tous ceux qui croient qu'un ordinateur ne pense pas et donc ne découvre pas. Même si l'ordinateur IBM n'a pas eu conscience de sa découverte, je crois qu'il faut avoir un peu plus de considération et d'estime pour cette nouvelle espèce à laquelle nous donnons naissance et qui nous rend tant de services.

Les derniers records mentionnés dans la table proviennent du projet GIMPS qui, avant le succès de N. Hajratwala, avait déjà découvert trois nombres premiers de Mersenne grâce aux ordinateurs de Joël Armengaud (novembre 1996), de George Spence (août 1997), et de Roland Clarkson (janvier 1998). Ce dernier est un jeune étudiant de 19 ans dont l'ordinateur a découvert la primalité de $M_{3021377}$, un nombre de 909 526 chiffres.

UN MÉCÈNE DONNE UN DEMI-MILLION DE DOLLARS

Ces premières découvertes furent faites uniquement pour la beauté de l'art, car c'est seulement en mars 1999 que le prix dont nous avons parlé a été créé par l'EFF. L'*Electronic Frontier Foundation* est une association de défense et de promotion de l'utilisation de l'Internet. À la suite du don d'un mécène anonyme, un prix de 50 000 $ (environ 300 000 F) a été promis au premier individu ou groupe qui découvrirait un nombre premier de plus de un million de chiffres décimaux. C'est ce prix que N. Hajratwala vient de gagner ; 100 000 $ récompenseront la découverte du premier nombre premier de plus de dix millions de chiffres décimaux, 150 000 $ la découverte du premier nombre premier de plus de 100 millions de chiffres décimaux, et 250 000 $ le premier nombre premier de plus d'un milliard de chiffres décimaux. Soit un total d'un demi-million de dollars si vous gagnez tous les prix d'un coup.

Les règles précises de ce concours sont intéressantes (démonstrations contrôlables, calculs reproductibles, publications reconnues, confirmations par des experts), car elles traduisent ce qu'on sait aujourd'hui sur la génération des nombres premiers, sur les formules pour créer des nombres premiers et sur les preuves de primalité. Ces règles intéresseront les amateurs qui, persuadés d'avoir trouvé des résultats importants sur les nombres premiers, s'interrogent sur la façon de faire reconnaître et valider leurs découvertes.

Les organisateurs du concours demandent que tout prétendant à l'un des prix fournisse une définition précise du nombre gagnant : pas question de proposer un nombre en disant que c'est la solution d'un système de 100 équations compliquées, même si l'on précise lesquelles ! Le prétendant doit aussi indiquer la méthode de preuve qui assure la primalité du nombre proposé, laquelle doit pouvoir être mise en œuvre par d'autres chercheurs.

Les tests de primalité probabilistes (qui indiquent qu'un nombre est premier avec une probabilité de 99,99 pour cent, par

6. LA FORMULE DE MARCEL PAGNOL

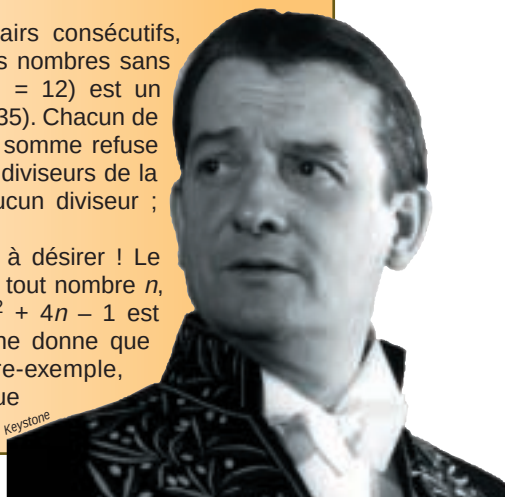
En 1992, Jacqueline et Frédéric Pagnol ont publié le texte de notes inédites que leur époux et père, le grand écrivain Marcel Pagnol, avait laissées. L'ouvrage, paru aux Éditions Pastorelly, porte le titre paradoxal *Inédits* et contient quelques pages sur les nombres premiers que l'amateur de mathématiques qu'était Marcel Pagnol avait soigneusement conservées. L'éditeur, dans un court texte de présentation, précise que "le conteur merveilleux est aussi un mathématicien rigoureux qui s'attaque aux problèmes les plus ardus, tels que les nombres premiers". Conscient peut-être de ce que ses notes comportaient un aspect conjectural et risqué, Pagnol les avait gardées pour lui. Leur naïveté étonne et "nous fend le cœur". En voici le texte, qui m'a été signalé par Paul Perbost.

«Quoique je ne sois pas mathématicien, j'aime les chiffres et les nombres, et surtout les nombres premiers qui sont assez mystérieux. Je crois avoir trouvé une formule qui permet de fabriquer des nombres premiers : c'est la petite équation suivante. x et $(x + 2)$ sont deux impairs consécutifs, comme 5 et 7 ou 17 et 19, etc. $x + (x + 2) + x(x + 2) =$ premier ; $(5 + 7) + (5 \times 7) = 47$. C'est-à-dire que la somme de deux impairs consécutifs et de leur produit est un premier. Nous avons donc une formule qui nous permet de construire des nombres premiers, et un moyen très simple de confirmer l'exactitude de nos calculs. $15 + 17 + 15 \times 17 = 287$ premier.»

Si Pagnol avait essayé 9 et 11, il aurait trouvé que $9 + 11 + 9 \times 11 = 119 = 7 \times 17$. Suivent d'autres exemples et calculs, où étrangement Marcel Pagnol semble prouver que, pour $x = 55$, le nombre obtenu par sa formule, 3 247, est premier alors que pourtant $3\,247 = 17 \times 191$. Pagnol entreprend de démontrer sa formule.

«Pourquoi la première formule, de deux impairs consécutifs, nous donne-t-elle des premiers, c'est-à-dire des nombres sans diviseurs? C'est parce que la somme $(5 + 7 = 12)$ est un nombre pair, et le produit est un impair $(7 \times 5 = 35)$. Chacun de ses nombres a son (ou ses) diviseur(s). Or, la somme refuse les diviseurs du produit, et le produit refuse les diviseurs de la somme, et le total des deux n'admet donc aucun diviseur ; c'est donc un nombre premier.»

Vous conviendrez que ce raisonnement laisse à désirer ! Le théorème que M. Pagnol propose est que, pour tout nombre n, $(2n - 1) + (2n + 1) + (2n + 1)(2n - 1) = 4n^2 + 4n - 1$ est premier. On sait prouver qu'aucun polynôme ne donne que des nombres premiers. Même sans contre-exemple, Pagnol, s'il avait connu ce résultat, aurait su que sa conjecture était fausse.


Keystone

exemple) sont exclus par les organisateurs. Je trouve cette option discutable, car un test probabiliste fait de telle façon qu'il ne reste qu'une probabilité d'erreur inférieure à 10^{-1000} serait aussi sûr qu'un test fait (même plusieurs fois) sur des machines qui ont chacune une probabilité de mauvais fonctionnement supérieure à 10^{-100}. Cette clause n'est toutefois pas pénalisante, car les tests probabilistes ne savent pas traiter efficacement des nombres de plusieurs millions de chiffres.

Il n'est pas impossible et pas interdit par les règles du concours EFF que quelqu'un réclame le prix en proposant non pas un long calcul, mais une formule facilement exploitable *f(n) (voir l'article de janvier 1999 de cette rubrique sur les formules pour les nombres premiers)* avec la démonstration mathématique que, pour toute valeur du paramètre n, la formule $f(n)$ produit un nombre premier.

Si, par exemple, la formule de Marcel Pagnol $4n^2 + 4n - 1$ avait été correcte, comme c'est une formule simple à mettre en œuvre pour obtenir des nombres de un million, dix millions, cent millions, et même un milliard de chiffres, le grand écrivain aurait pu (aidé d'un informaticien pour expliciter les développements décimaux de ses propositions) réclamer d'un coup tous les prix offerts par l'EFF. Si vous détenez une telle formule, vous êtes riche.

Pour qu'un prétendant gagne un prix, l'annonce de son résultat, avec un minimum de précisions sur la méthode permettant de prouver la primalité, doit être publiée dans une revue académique. De telles revues procèdent à l'expertise préalable des articles publiés en les soumettant à des spécialistes reconnus. Même si l'article rendant compte du record ne comporte qu'une seule page, il assure que le prix est attribué en accord avec les expertises scientifiques.

Si vous proposez une formule nouvelle, l'article devra comporter la preuve qu'elle donne des nombres premiers et des indications sur son exploitation concrète pour engendrer des nombres premiers de un million de chiffres ou plus. Si quelqu'un proposait une formule simple dont la démonstration qu'elle ne donne que des nombres premiers est complexe (il est fréquent en arithmétique que les démonstrations occupent des dizaines de pages), la vérification pourrait prendre plusieurs mois.

Les organisateurs se réservent la possibilité de demander le développement décimal complet des nombres proposés. Expliciter ce développement décimal pour une formule du genre $3^{1000000} + 17$ n'est pas très facile, mais les spécialistes y arrivent pour des nombres de quelques millions de chiffres, voire quelques milliards de chiffres. Si votre proposition est simple, on ne vous demandera pas d'en expliciter le développement décimal ; si elle est inhabituelle, alors il faudra que vous prouviez que vous êtes capable de l'exploiter. Si vous avez trouvé une méthode, vous réussirez sans peine à convaincre un spécialiste de vous aider… contre une partie de la récompense.

7. LES DIVISEURS PREMIERS DE M_p

Il est plus facile de démontrer que les nombres de Mersenne sont premiers que d'autres nombres, car un diviseur premier de $2^p - 1 = M_p$ (p premier supérieur à 2) est toujours de la forme $2mp + 1$.
En effet, soit q un diviseur premier de $2^p - 1 = M_p$ (p premier et > 2).
On a : $2^p - 1 = 0 \pmod q$, donc $2^p = 1 \pmod q$.
Les solutions positives de l'équation $2^x = 1 \pmod q$ sont les multiples d'un nombre positif, k, plus petite solution positive de l'équation $2^x = 1 \pmod q$ (cela résulte du fait évident que, si x et x' sont deux solutions positives de cette équation, leur différence aussi).
Le plus petit k tel que $2^k = 1 \pmod q$ est donc un diviseur de p, c'est-à-dire 1 ou p. Ce ne peut pas être 1, car $2^1 \neq 1 \pmod q$, c'est donc p.
En utilisant le petit théorème de Fermat (qui dit que, si q est premier, alors pour tout nombre a qui n'est pas multiple de q, il existe un q positif tel que $a^k = 1 \pmod q$) et que le plus petit k positif vérifiant cette équation divise $q - 1$), on en déduit que p divise $q - 1$, autrement dit $q = hp + 1$ pour un certain h. Ce nombre h est pair, car sinon hp serait impair et donc q serait pair, ce qui ne se peut pas puisque q est un diviseur premier d'un nombre impair. Donc $h = 2m$, et donc $q = 2mp + 1$.
Ce théorème permet de déterminer rapidement les M_p qui sont premiers. Ainsi, pour étudier la primalité de $M_{13} = 2^{13} - 1 = 8\,091$, il suffit de tester si ce nombre est divisible par un nombre premier de la forme $26k + 1$ inférieur à $\sqrt{8091} = 90{,}504$. Les nombres de la forme $26k + 1$ inférieurs à 91 sont 27, 53 et 79. Seuls 53 et 79 sont premiers. Deux divisions suffisent pour prouver que M_{13} est premier.

UN MARCHÉ DU CALCUL?

Les promoteurs pourraient développer ainsi un marché du temps de calcul. D'une part, chaque propriétaire d'une machine (même de puissance moyenne) n'utilise que très peu la puissance de sa machine et, si on lui proposait quelques francs par jour pour que sa machine travaille quand il ne s'en sert pas, il serait heureux et gagnant (en quelques mois, il récupérerait le prix d'achat de sa machine). D'autre part, de nombreux projets scientifiques pourraient bénéficier de l'existence de ce marché qui éviterait le gâchis formidable de 99 pour cent de la capacité de calcul dont dispose l'humanité.

Des projets fonctionnant aujourd'hui sur le principe du bénévolat ont déjà été mis en place (le projet GIMPS dont nous avons parlé ci-dessus en est un exemple). Ces calculs géants en réseaux auxquels chacun peut associer sa machine portent sur la factorisation de grands entiers, sur la recherche des chiffres binaires de π, sur l'étude détaillée de signaux radio provenant du ciel pour y découvrir d'éventuels signes d'intelligence extraterrestre (projet SETI), sur le craquage de codes cryptographiques créés par défi ou par des firmes qui veulent montrer qu'elles vendent des méthodes résistant aux attaques les plus sérieuses.

Le réseau Internet pourrait changer l'univers de l'information, mais aussi l'univers du commerce. Avec les projets de calculs distribués, il pourrait aussi bouleverser l'univers du calcul pour atteindre des puissances de calcul aujourd'hui réservées aux riches institutions. Il se pourrait aussi que la loi de Moore (doublement de la puissance de calcul tous les 18 mois) puisse par ces moyens être dépassée (doublement tous les 12 mois, voire tous les 6 mois).

Jean-Paul DELAHAYE est professeur d'informatique à l'Université de Lille.

http://www.mersenne.org/prime.html : The Great Internet Mersenne Prime Search. Pour participer à la recherche de nouveaux nombres premiers records.

http://entropia.com : organisation dédiée à des projets de calculs distribués.

http://eff.org et http://eff.org/coopawards/ : à propos des prix proposés par l'Electronic Frontier Foundation.

http://www.scruznet.com/~luke/mersenne.htm : à propos de Marin Mersenne.

http://www.utm.edu/research/primes/ Le meilleur site internet sur les nombres premiers (C. Caldwell).