

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 d'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

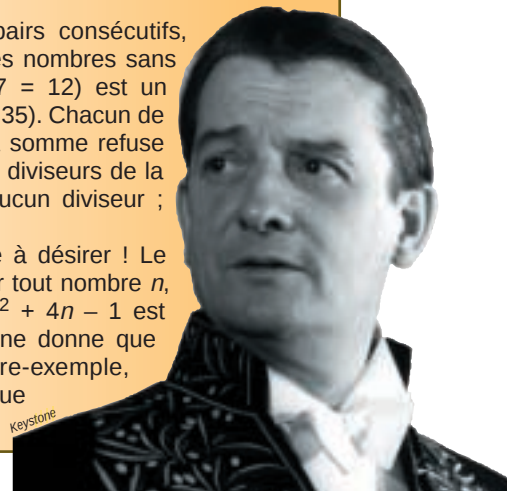
En 1992, Jacqueline et Frédéric Pagnol ont publié le texte de notes inédites que leur époux et père, le grand écrivain Marcel Pagnol, avait laissées. L'ouvrage, paru aux Éditions Pastorelly, porte le titre paradoxal *Inédits* et contient quelques pages sur les nombres premiers que l'amateur de mathématiques 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 ardu, 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.



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,

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 : $2^p - 1 \equiv 0 \pmod{q}$, donc $2^p \equiv 1 \pmod{q}$.

Les solutions positives de l'équation $2^x \equiv 1 \pmod{q}$ sont les multiples d'un nombre positif, k , plus petite solution positive de l'équation $2^x \equiv 1 \pmod{q}$ (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 $2^k \equiv 1 \pmod{q}$ est donc un diviseur de p , c'est-à-dire 1 ou p . Ce ne peut pas être 1, car $2^1 \not\equiv 1 \pmod{q}$, 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 $a^q \equiv 1 \pmod{q}$) 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.

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.

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/coop-awards/> : 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).