

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 :

$$X^n - 1 = (X - 1)(X^{n-1} + X^{n-2} + \dots + X^2 + X + 1)$$

qui, en prenant $X = 2^a$ et $n = b$, donne :

$$2^p - 1 = 2^{ab} - 1 = (2^a)^b - 1 = (2^a - 1)((2^a)^{b-1} + (2^a)^{b-2} + \dots + (2^a) + 1).$$

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 xvi^e 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 xvi^e 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 suspects 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 $k < 2^n$ et s'il existe un nombre entier a tel que : $a^{(N-1)/2} + 1 \equiv 0 \pmod{N}$, 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 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.

