

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, $p = a \cdot b$ 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 $N = k \cdot 2^n + 1$ 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.