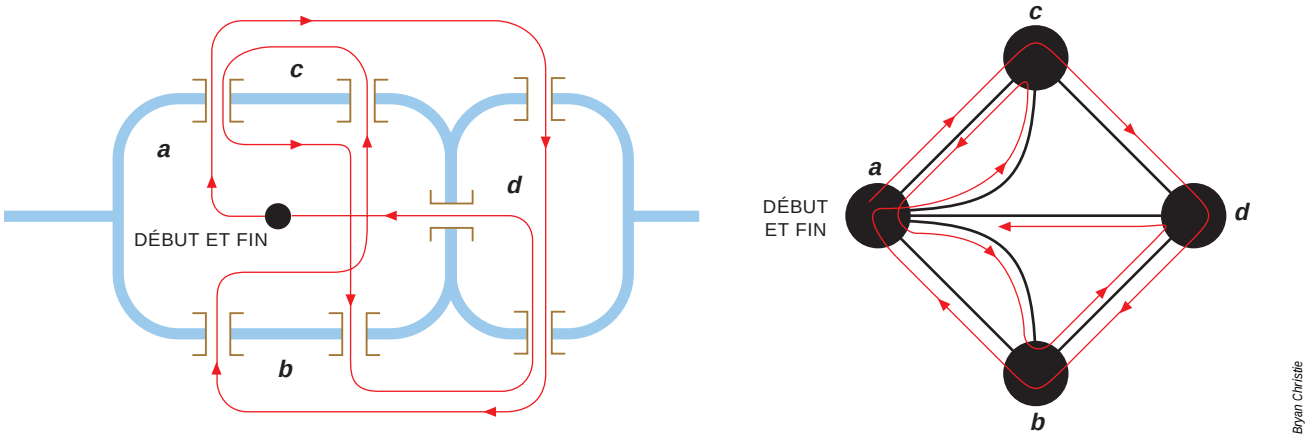



**2. Le problème des sept ponts de Königsberg et son graphe : les points noirs représentent les masses terrestres, et les arêtes noires, les ponts.**

huit faces triangulaires. Une danse encore plus complexe commence avec une seule longue boucle tenue par trois personnes : la boucle a d'abord une forme de triangle, mais elle est ensuite transformée en tétraèdre, puis en octaèdre (un solide à huit faces triangulaires). Puis un quatrième danseur se joint au groupe et participe à la transformation de l'octaèdre en cube. Enfin six danseurs viennent déformer le cube pour obtenir un dodécaèdre (à 12 faces pentagonales), puis un icosaèdre (20 faces triangulaires). Les cinq solides platoniciens (les polyèdres réguliers que sont le tétraèdre, le cube, l'octaèdre, le dodécaèdre et l'icosaèdre) sont ainsi tous représentés.

Ces danses avec des figures de ficelle posent des problèmes qui se rapprochent de ceux qui ont engendré la topologie. Quelles arêtes des polyèdres réalisés doivent-elles être doublées, par exemple? Ce type de question s'analyse en termes de «cycles eulériens» dans les graphes. Un graphe est un ensemble de points, ou sommets, reliés par des segments, ou arêtes. Un cycle eulérien est un chemin fermé, ou circuit, qui passe une fois et une seule par toutes les arêtes du graphe (on ne le confondra pas avec un circuit hamiltonien, qui passe une fois et une seule par chaque sommet). On peut représenter une danse par un graphe si l'on fait correspondre des sommets aux mains des participants, et des arêtes aux parties de ficelle qui forment les polyèdres. Certaines des arêtes de polyèdres sont composées de plusieurs brins de ficelle. Pourquoi? Les danseurs peuvent-ils former les polyèdres avec seulement un brin de ficelle par arête?

Généralement non. Supposons que l'on forme un polyèdre en n'utilisant qu'une boucle de ficelle. Celle-ci forme un cycle qui passe par tous les sommets du polyèdre. Or, en 1735, le mathématicien suisse Leonhard Euler rencontra une structure analogue quand il étudia le problème des sept ponts de Königsberg : la ville de Königsberg (aujourd'hui Kaliningrad, en Russie) est construite sur une rivière, la Pregel, et comprend deux îles. À l'époque d'Euler, sept ponts reliaient les îles aux rives ou entre elles *(voir la figure 2)*. On raconte que les habitants avaient cherché pendant longtemps un circuit passant sur chacun de ces ponts une fois et une seule. Euler démontra qu'un tel circuit n'existait pas.

Comment obtint-il ce résultat? Il considéra d'abord les quatre masses terrestres – les deux îles *(a* et *d)* et les deux rives *(b* et *c)* –, qu'il associa aux sommets d'un graphe ; puis il associa les sept ponts à des arêtes entre ces sommets. Ayant ainsi transformé le problème en un problème de théorie des graphes, Euler montra que si une boucle passe une fois et une seule par chaque arête, alors un nombre pair d'arêtes arrive à chaque sommet. En effet, comme le chemin considéré est un cycle, chaque fois que la boucle arrive à un sommet par une arête, elle doit le quitter par une autre arête. Les arêtes sont ainsi appariées, et le nombre total d'arêtes reliées à chaque sommet est pair. Cette condition de parité n'est pas vérifiée à Königsberg où, à chaque «sommet», arrivent des arêtes en nombre impair (trois ou cinq, selon les sommets).

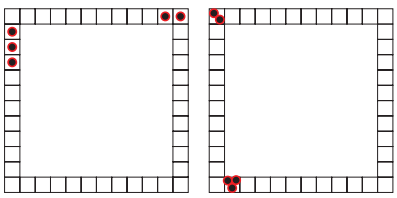
Euler fit mieux, en démontrant le résultat réciproque : dans tout graphe connexe (c'est-à-dire d'un seul tenant) où chaque sommet est relié à un nombre pair d'arêtes, il existe un circuit qui passe par chaque arête une fois et une seule. Ce théorème explique les arêtes doublées dans les danses avec de la ficelle.

Considérons, par exemple, le dodécaèdre, à 20 sommets reliés par 30 arêtes. Comme trois arêtes (un nombre impair) arrivent à chaque sommet, il n'existe pas de circuit qui passe par chaque arête une fois et une seule. En revanche, quand une de ces trois arêtes est «doublée», quatre arêtes (un nombre pair) arrivent à chaque sommet. Pouvez-vous identifier dix arêtes telles que, si on les double, quatre arêtes arrivent à chaque sommet? Sinon, vous pourriez les doubler toutes : six arêtes arriveraient alors à chaque sommet. Mais un si grand nombre est-il nécessaire?

Comme cet exemple le montre, les danses avec des figures de ficelle peuvent constituer d'instructives introductions à la géométrie dans l'espace à trois dimensions. Ce sont aussi des jeux très amusants : essayez-les la prochaine fois que vous serez dans une réunion ennuyeuse.

## Réactions

Dans mon article intitulé *Chœurs lumineux* (*Pour la Science*, mai 1999), je demandais si, dans le Jeu du flash, on pourrait trouver des configurations qui, au lieu d'évoluer vers un synchronisme des lucioles, aboutiraient à des cycles, les jetons étant répartis sur plusieurs cases. Cette situation n'a pas lieu dans le modèle mathématique de la synchronisation des lucioles, mais elle se rencontre dans le Jeu du flash, qui est discontinu. William Evans, d'Irvine, a découvert que si le damier a douze cases de côté, avec cinq lucioles, une position initiale *(ci-dessous à gauche)* évolue, après 27 coups, vers une seconde configuration *(à droite)* qui se répète avec une période égale à 38 coups.



# 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 $2^n - 1$. Ces nombres intéressent les mathématiciens depuis longtemps, et celui-ci est le 38e 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'impiété 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

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.