

nous l'avons dit, d'obtenir de «bonnes solutions». Dans l'exemple du compteur de vitesse, la méthode suivie par le graveur de cadran a été la suivante : il a commencé par tracer la courbe donnant la position de l'aiguille pour certaines valeurs de la vitesse et a ainsi obtenu un modèle direct. Puis il s'est posé la question : «Pour chaque position de l'aiguille, quelle est la valeur de la vitesse qui, appliquée au modèle, créerait un déplacement identique du mouvement réel?» Il a ensuite porté ces indications de vitesse pour chacune des positions.

Ainsi, lorsqu'on applique les «bonnes valeurs» des inconnues à l'entrée du modèle direct, le calcul doit fournir des observations «synthétiques» les plus proches possibles des observations réelles : c'est le critère de conformité aux observations. Pour les cas simples, tel le compteur de vitesse, observations réelles et observations synthétiques peuvent être égales.

Dans les systèmes très incertains ou quand le nombre des observations est différent de celui des grandeurs recherchées, la conformité absolue aux observations est impossible. Dans le cas des problèmes mal posés, la conformité aux observations ne permet pas d'obtenir une solution unique (du moins, avec une précision suffisante). On ajoute alors un second critère : les observations synthétiques doivent être aussi proches que possible de ce que l'on en savait avant de faire la mesure. C'est un critère de conformité à l'information *a priori*.

Dans le cas général, on définit un critère composite, formé d'un critère de conformité aux observations (distance entre les observations et les sorties du modèle, ou observations synthétiques) et d'un critère de conformité à l'information *a priori*. Les «bonnes valeurs» des inconnues sont celles qui minimisent ce critère composite. Dans la pratique, on utilise un algorithme numérique qui effectue des itérations en proposant des solutions successives jusqu'à ce que le critère composite soit minimisé.

## La mesure de l'information gagnée

Lorsqu'un ingénieur adopte la démarche que nous venons d'exposer afin de résoudre un problème de mesure particulier, il est conduit à effectuer des choix à plusieurs niveaux de la chaîne de mesure. Ainsi, nous avons vu que la

qualité des mesures dépend du modèle choisi. Plus généralement, on peut énoncer un critère informationnel de la qualité d'une méthode de mesure, qui guidera l'ensemble des choix.

Supposons que l'on fasse la mesure d'une tension comprise entre 0 et 256 volts avec un convertisseur analogique-numérique parfait à 256 niveaux de quantification : un tel appareil transforme une tension analogique, c'est-à-dire variant continûment, en une tension choisie parmi 256 valeurs numériques (ici, chaque niveau de quantification a donc une largeur de un volt). Avant de faire la mesure, on sait que la tension sera toujours comprise entre 0 et 256 volts : c'est l'information *a priori*. Après la mesure, si l'appareil affiche par exemple 123 volts, on sait que la tension était comprise entre 122,5 volts et 123,5 volts : c'est l'information *a posteriori*. La mesure a divisé l'incertitude par 256, et l'on peut alors calculer l'«incrément d'information», qui traduit la différence entre l'information *a posteriori* et l'information *a priori*, exprimées par des fonctions de densité de probabilité. Cet incrément est mesuré en bits : il est ici égal à 8 bits ( $2^8 = 256$ ).

La notion d'incrément d'information caractérise ainsi de façon quantitative la qualité d'une mesure, ou d'un système de mesure (ensemble de l'appareillage et des algorithmes utilisés). Plus cet incrément est grand, meilleure est la mesure.

L'incrément d'information dépend évidemment de l'instrument de mesure. Celui-ci est en partie caractérisé par un certain nombre de paramètres : le nombre et les valeurs des fréquences dans le cas du zinc, le nombre et la position des capteurs de rayonnement dans le cas de la tomographie en rayons X, ou encore le nombre de personnes interrogées dans un sondage. On peut alors optimiser ces paramètres, appelés instrumentaux, soit en maximisant l'incrément d'information pour un nombre d'observations donné, soit en minimisant le nombre d'observations pour une incertitude résiduelle donnée, ce dernier cas se traduisant évidemment par une diminution de la complexité, donc du coût, du système de mesure.

Toutefois, à l'exception, heureusement courante, de quelques cas simples (systèmes linéaires et incertitudes réparties selon une fonction de Gauss, suivant une courbe «en

cloche»), l'incrément d'information ne peut être déterminé que par des méthodes approximatives et lourdes, tandis que les biais induits par certaines non linéarités ne peuvent être pris en compte par des méthodes analytiques. Toutes ces raisons créent des difficultés pratiques qui font que la notion d'incrément d'information, la seule conforme à une définition «informationnelle» de la mesure, reste rarement utilisée (sauf dans le cas des sondages et, plus généralement, des statistiques, où sa mise en œuvre est évidente). Notre équipe a mis au point des méthodes d'évaluation statistiques pour remédier à cette difficulté. Dans les cas très complexes, plusieurs autres méthodes existent, telles celles qui cherchent à minimiser le caractère mal posé du problème.

C'est ce que nous avons fait pour la mesure de l'épaisseur du zinc, en optimisant le choix des fréquences de travail (c'est l'optimisation de l'instrument). Cette optimisation a permis de choisir quelques fréquences pour lesquelles les mesures de l'impédance de la bobine autorisent la détermination (par la minimisation d'un critère de conformité aux observations et à l'information *a priori*) d'un triplet d'inconnues unique (à des incertitudes raisonnables près, c'est-à-dire du même ordre de grandeur que celles présentes sur les mesures d'impédance).

---

Jacques OKSMAN dirige le Service des mesures à l'École supérieure d'électricité, à Gif-sur-Yvette.

A. TARANTOLA, *Inverse Problem Theory- Methods for Data Fitting and Model Parameter Estimation*, Elsevier, 1987.

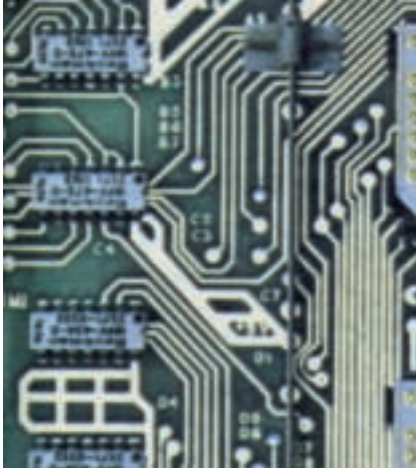
E. WALTER et L. PRONZATO, *Outils et méthodes pour la reconstruction de modèles paramétriques à partir de données expérimentales*, Masson, 1994.

L. LE BRUSQUET et J. OKSMAN, *Débit-métrie par traceurs : reconstruction du profil de concentration*, 1<sup>er</sup> Colloque interdisciplinaire en instrumentation, pp. 531-538, 18-19 novembre 1998.

L. SANDU, J. OKSMAN et G. FLEURY, *Information Criteria for the Choice of Parametric Functions for Measurement*, in *IEEE Transactions on Measurement*, à paraître.

M. DAVOUST, G. FLEURY et J. OKSMAN, *A Parametric Estimation Approach for Grooves Dimensioning using Remote Field Eddy Current Inspection*, in *Research in Nondestructing Evaluation*, à paraître.

---



# Graphes et électronique

IAN STEWART

*Comment tester les circuits imprimés.*

Le coloriage, un jeu d'enfant ? Détrompez-vous : de nombreux mathématiciens ont cherché à démontrer que quatre couleurs seulement permettent de colorier toutes les cartes de sorte que les pays voisins soient de couleurs différentes, et c'est seulement un superordinateur qui a fini le travail : il a examiné un à un les nombreux cas qui restaient après l'analyse strictement mathématique du problème. Le plus fascinant de l'histoire, c'est que des résultats mathématiques voisins, à propos de coloriages, ont des applications inattendues... en électronique.

Les objets mathématiques utiles sont cette fois des graphes, composés de sommets reliés par des lignes nommées arcs ou arêtes. L'«épaisseur» d'un graphe, notamment, est un concept découvert par

des chercheurs des Laboratoires AT&T Bell, à Murray Hill, qui a été utilisé en électronique par Joan Hutchinson, du Collège Malacaster, dans le Minnesota.

Commençons par une définition : un graphe est planaire, ou d'épaisseur égale à un, s'il peut être dessiné sur un plan, sans que ses arcs se recoupent. Les graphes d'épaisseurs égale à deux sont ceux dont les arcs doivent être groupés en deux ensembles planaires. De même, les graphes d'épaisseur égale à trois ont des arcs qui sont groupés en trois ensembles planaires, etc.

Ainsi un graphe d'épaisseur égale à deux est comme un sandwich : une des tranches de pain porte les arcs du premier ensemble, qui ne se coupent jamais ; l'autre tranche porte les arcs du second ensemble, qui ne se coupent pas non plus. Les sommets étirés en segments verticaux forment en quelque sorte la garniture du sandwich (voir la figure 1).

De même, un circuit imprimé est analogue à un graphe dont les sommets sont les composants électroniques, et dont les arcs sont les connexions électriques entre les composants. Idéalement, les fabricants cherchent à réaliser des circuits imprimés planaires, sans fils chevauchant les pistes conductrices. Avec les cartes à double face, ils réalisent des graphes d'épaisseur égale à deux. Pour réaliser des circuits associés à des graphes d'épaisseur supérieure, plus d'un circuit imprimé s'impose. Ce même genre de considérations se retrouve en micro-électronique, dans la fabrication des puces.

De nombreux circuits imprimés utilisés dans l'industrie sont des grilles de  $100 \times 100$  trous, où l'on fixe des composants, en les reliant par des pistes horizontales ou verticales faites d'un matériau conducteur. Les fabricants sont confrontés au difficile problème de la détection des cartes défectueuses, où des parties de pistes relient des composants qui devraient être séparés.

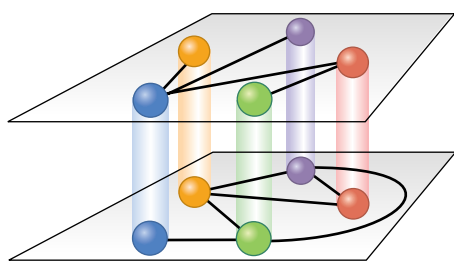
Pour des raisons pratiques, les fabricants groupent les composants d'un circuit imprimé en «maillages de pistes» : un

maillage est un ensemble de composants reliés par des pistes conductrices, sans boucle. Nous examinerons ici le problème de la recherche de courts-circuits, c'est-à-dire de connexions fautives. La méthode de test la plus simple est l'examen de toutes les paires de maillages : on connecte un maillage d'une paire testée au pôle positif d'une pile, et l'autre maillage au pôle négatif, via une ampoule. Si les maillages sont connectés, le courant électrique passe dans la lampe, qui s'allume (dans l'industrie électronique, les appareils de tests sont automatiques).

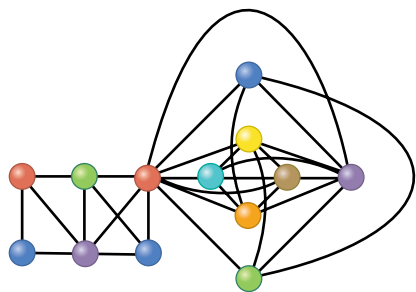
Toutefois, pour des circuits à  $n$  maillages, cette méthode nécessite  $n(n-1)/2$  tests (c'est le nombre de paires de maillages). Avec des circuits imprimés qui comportent quelque 500 maillages, il faut 125 000 tests par carte, ce qui est excessif. La simple application du concept d'épaisseur d'un graphe réduit le nombre de tests à 11 ! Et, même, avec un peu de réflexion, à seulement 4.

Commençons par construire un graphe qui puisse décrire les courts-circuits : le «graphe de maillages» du circuit. Comme nous cherchons des courts-circuits entre des maillages, nous assignons un sommet à chaque maillage. Les arcs représentent alors les courts-circuits potentiels (pas les courts-circuits existants, bien sûr : si nous savions où ils se trouvent, nous n'aurions pas à les chercher). Plus précisément, deux sommets du graphe de maillages sont joints par un arc chaque fois que les maillages correspondants sont «adjacents», c'est-à-dire qu'ils peuvent être connectés par une droite horizontale ou verticale, qui ne traverse aucun maillage intermédiaire.

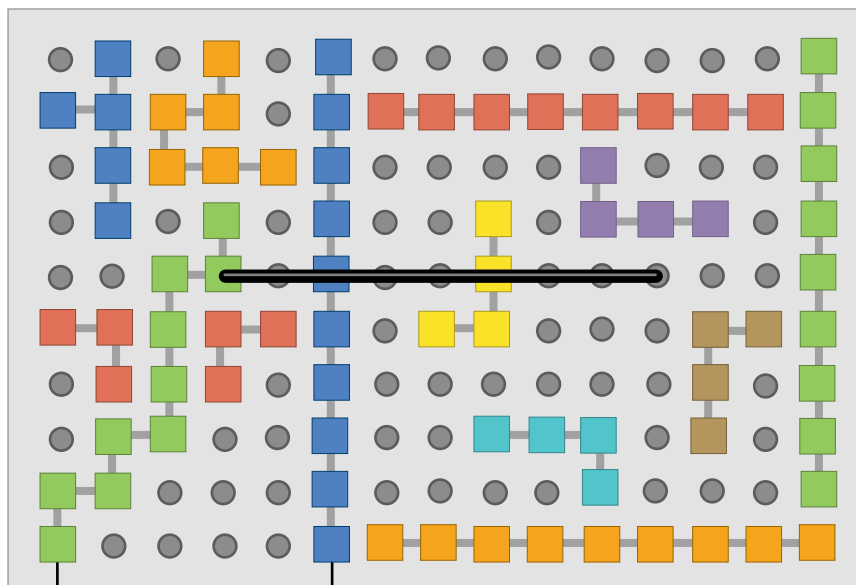
En principe, on peut imaginer des courts-circuits entre des maillages qui ne sont pas adjacents, mais des maillages adjacents seraient alors court-circuités et nous les dépisterons si nous identifions les jonctions entre les maillages adjacents. En effet, le robot de fabrication passe deux fois sur le panneau : une fois pour déposer les



1. Ce sandwich représente un graphe d'épaisseur égale à deux : il est composé de deux graphes planaires dont les sommets respectifs ont été étirés en segments verticaux.



2. Le graphe de maillages du circuit imprimé de la figure 3 est d'épaisseur égale à deux (une unité pour chaque face de la carte). Chaque réseau y est représenté par un sommet ; les sommets adjacents sont reliés par des arcs : ce sont les courts-circuits potentiels.



connections horizontales, et une fois pour déposer les connections verticales. Des erreurs se produisent quand il dépose trop de matériau conducteur, reliant deux mailages qui devaient être séparés : si deux mailages non adjacents sont ainsi reliés, des mailages adjacents, entre eux, le seront nécessairement aussi.

Nous avons vu que le graphe d'une carte électronique est d'épaisseur égale à deux si les deux faces comportent un circuit imprimé. Le graphe de mailages, pour la même raison, est aussi d'épaisseur égale à deux. Or le mathématicien britannique Percy John Heawood a démontré, au XIX<sup>e</sup> siècle, que tout graphe d'épaisseur égale à deux peut être «12-colorié» : avec 12 couleurs, on peut colorier les sommets de sorte que deux sommets joints par un arc soient toujours de couleurs différentes. Ainsi le graphe de mailages de tout circuit imprimé peut être 12-colorié, et nous pouvons transférer ce coloriage (conceptuellement) aux mailages des circuits imprimés. Avec 12 couleurs, on peut donc associer une couleur à chaque mailage, de sorte que deux mailages de la même couleur ne soient jamais adjacents. Comme nous cherchons les courts-circuits entre des mailages adjacents, nous pouvons restreindre nos recherches à des courts-circuits entre mailages de couleurs différentes.

Pour effectuer ces recherches, groupons tous les mailages de même couleur : pour chacune des 12 couleurs, nous construisons une «sonde», c'est-à-dire une structure arborescente réalisée en

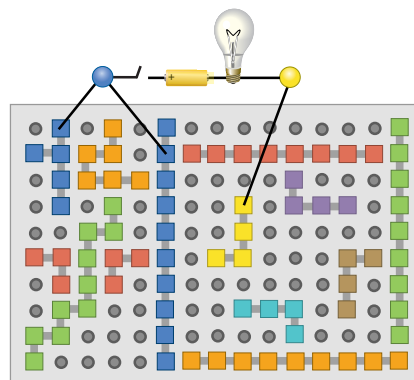
**3. Un circuit imprimé comporte des trous (cercles) où sont fixés les composants électroniques (carrés). Les composants sont reliés par des pistes métalliques en «mailages». Des mailages adjacents peuvent être représentés par des couleurs différentes. Des pistes anormales qui relient des pistes adjacentes (en noir) sont à l'origine de courts-circuits. Quand on relie un circuit composé d'une lampe et d'une pile en série aux mailages bleu et vert, le courant électrique passe dans la lampe, qui s'allume.**

matériau conducteur et qui relie tous les mailages d'une même couleur.

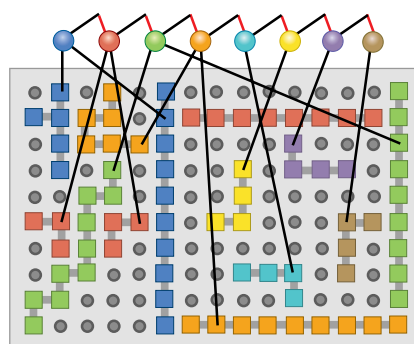
Par exemple, relierons tous les mailages bleus ensemble, d'une part, et tous les mailages jaunes, d'autre part. Puis relierons ces groupes par l'intermédiaire d'un circuit composé d'une pile et d'une ampoule en série : si le circuit n'est pas défectueux, aucun courant ne passe, car aucun des mailages bleus n'est relié aux mailages jaunes. Le courant ne passe que si une erreur de fabrication a relié un mailage bleu à un mailage jaune.

Ce test n'indique pas où se trouve les courts-circuits éventuels, mais cette information n'est pas utile : les fabricants de circuits imprimés jettent généralement les cartes défectueuses sans chercher à les réparer. Aussi, pour détecter la présence d'un défaut, il suffit de tester toutes les paires possibles de sondes. Au lieu de 125 000 tests, 66 suffisent.

**O**n peut même faire mieux. Testons les groupes de mailages de couleur 1 et de couleur 2 ; rejetons les cartes défectueuses. Puis, relierons ensemble les groupes de mailages de couleurs 1 et 2, et cherchons si cet ensemble est relié au groupe de mailages de couleur 3 : si la lampe s'allume, c'est la preuve que le groupe de mailages de couleur 3 est relié au groupe de mailages de couleur 1 ou au groupe de mailages de couleur 2. Or



**4. On teste efficacement les circuits imprimés si l'on cherche des courts-circuits entre groupes de mailages d'une même couleur. En plaçant une ampoule et une pile entre les groupes de mailages bleu et jaune, on détecte un éventuel court-circuit entre les mailages de ces couleurs.**



**5. On réduit encore le nombre de tests en connectant des groupes de mailages.**

chacune de ces deux éventualités conduit à un défaut, qui nous conduit à rejeter la carte. Nous poursuivons alors les regroupements et les tests : ainsi le nombre de tests est réduit à 11.

Allen Schwank, de l'Université du Michigan, a encore réduit ce nombre. Il écrit d'abord les nombres 1, 2, ..., 12 en binaire : de 0001 à 1100 ; puis il repère chaque groupe de mailages par un de ces nombres. Il construit un «supergroupe» composé de tous les groupes dont le numéro commence par 0 et un autre supergroupe composé des groupes dont le numéro commence par 1. Il cherche si ces supergroupes sont connectés, et élimine les cartes où ils le sont. Pour les autres, il réalise deux nouveaux supergroupes entre les groupes ayant le même deuxième chiffre dans leur numérotation binaire, et il examine leur éventuelle connexion. Sinon il répète l'opération pour les troisièmes chiffres binaires, puis pour les quatrièmes. Et le travail s'achève ainsi. Pour comprendre la méthode, notons que si deux groupes distincts sont reliés par un court-circuit, leur indexation binaire doit différer par au moins un de leurs quatre chiffres ; de ce fait, un des quatre tests doit détecter les courts-circuits.

Les coloriages, un jeu d'enfant ? Peut-être, mais l'industrie électronique a intérêt que ses ingénieurs s'amuse comme des enfants.





# Les chasseurs de nombres premiers

JEAN-PAUL DELAHAYE

*Nuit et jour, des centaines d'ordinateurs recherchent éperdument des nombres premiers.*

Dans le zoo des nombres, les mathématiciens ont identifié, il y a plus de deux mille ans, une espèce remarquable, les nombres premiers (comme 2, 3, 5, 7, 11, ...) qui ne sont multiples exacts que de 1 et d'eux-mêmes. Ces nombres sont aux entiers ce que les éléments sont aux composés chimiques, car tout nombre entier se décompose de façon unique en produit de facteurs premiers. Exemple :  $440 = 2 \times 2 \times 2 \times 5 \times 11$ .

L'esprit de sérieux s'est emparé du sujet, et des milliers de pages de mathématiques difficiles, voire très difficiles, ont été écrites sur cette espèce numérique qui ne sera jamais en voie d'extinction puisqu'elle est infinie et que, de toute façon, lorsqu'un nombre est premier, rien ne peut changer sa nature !

Les universitaires sont obsessionnellement attachés à la répartition des nombres premiers (quelle est la proportion moyenne des nombres premiers parmi

les nombres inférieurs à  $n$ ?) ; ils s'y cassent le nez depuis plus de cent ans (la conjecture de Riemann, qui donnerait des informations précises de répartition échappe obstinément à toutes les tentatives de preuve). Parallèlement, une secte d'amateurs est restée fidèle à la tradition des pythagoriciens qui furent sans doute les premiers à définir et à prêter attention aux nombres premiers, et à y chercher émerveillements et amusements.

Les membres pacifiques et tranquilles de cette secte examinent les sous-espèces de nombres premiers, mènent toutes sortes de calculs, lancent des défis sans cesse renouvelés qui résistent ou tombent, mais sont alors reformulés en défis plus forts ou plus absurdes. Le tout constitue un jeu à l'échelle planétaire qui s'épanouit sur Internet. Ces zoologues mathématiciens se sont particulièrement intéressés aux nombres premiers *repunits* et aux nombres premiers palindromes.

## LES REPUNITS

Les *repunits* sont des nombres constitués d'une chaîne de 1. Le nombre 11 est premier. En revanche, le nombre 111 ne l'est pas, car  $111 = 3 \times 37$ . De même, quatre "1" consécutifs ou cinq "1" ne constituent pas des nombres premiers :  $1111 = 11 \times 101$  et  $11111 = 41 \times 271$ . Plus loin,  $11...1$  (19 fois le "1") est premier comme l'est  $11...1$  (23 fois le "1"). D'où la question : quels sont les *repunits* premiers ?

Cette question est loin d'être simple, et personne aujourd'hui ne connaît de règles simples permettant de savoir systématiquement et rapidement quels sont les *repunits* premiers et quels sont les *repunits* composés. Notre ignorance n'est cependant pas complète, car on a découvert quelques propriétés des *repunits*.

– Pour être premier, un *repunit* doit nécessairement comporter un nombre premier de "1". En effet, si  $m$  divise  $n$  alors  $11...1$  ( $m$  fois) divise  $11...1$  ( $n$  fois). On le démontre en généralisant l'égalité  $111111111111 = 1111 \times 100010001$  (ce qui est facile).

– Un nombre *repunit* ne peut être ni un carré (comme  $25 = 5 \times 5$ ), ni un cube (comme  $27 = 3 \times 3 \times 3$ ), ni une puissance cinquième (comme  $32 = 2 \times 2 \times 2 \times 2 \times 2$ ). Les deux derniers résultats sont récents, et nul ne sait ce qui se passe pour les puissances autres que les multiples de 2, 3 et 5.

Les *repunits* de petites tailles (moins de 30 000 chiffres) susceptibles d'être premiers ont été étudiés soigneusement. On peut résumer ce qu'on sait en quelques mots :

–  $11...1$  ( $n$  fois le "1") est un nombre premier pour  $n = 2, 19, 23, 317$  (découvert par Hugh Williams en 1978), 1031 (découvert par Hugh Williams et Harvey Dubner en 1986).

– Aucune autre valeur de  $n$  inférieure à 30 000 ne donne de *repunits* premiers. Au-delà de 30 000, les calculs deviennent trop longs, et l'on ignore donc ce qui s'y passe, comme d'ailleurs on ignore si l'espèce des *repunits* premiers est infinie.

## 1. REPUNITS EN BASE 2 ET NOMBRES DE MERSENNE

En base 2, les *repunits* sont de la forme  $2^n - 1$ . Ces nombres premiers sont dénommés les nombres premiers de Mersenne, en l'honneur du père Mersenne, qui les étudia en 1644.

Ces nombres sont particulièrement intéressants, car on connaît une méthode très efficace pour en tester la primalité. Le test de Lucas-Lehmer est basé sur le résultat suivant :  $2^p - 1$  est premier si et seulement si  $2^p - 1$  divise  $S(p - 1)$ , où  $S(1) = 4$  et  $S(n + 1) = S(n)^2 - 2$ .

Grâce à ce test, le plus grand nombre premier connu est un nombre de Mersenne. Il s'agit de  $2^{3021377} - 1$  (découvert en 1998 par Clarkson, Woltman et Kurowski), qui comporte 909 526 chiffres. On espère trouver un nombre premier de un million de chiffres avant l'an 2000.

On connaît aujourd'hui 37 nombres premiers de Mersenne, qui sont ceux correspondant aux exposants : 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253, 4423, 9689, 9941, 11213, 19937, 21701, 23209, 44497, 86243, 110503, 132049, 216091, 756839, 859433, 1257787, 1398269, 2976221, 3021377. On ne sait prouver que les nombres de Mersenne premiers sont en nombre infini, ni que les nombres de Mersenne composés ayant un exposant premier sont en nombre infini.