Les nombres parfaits

Marin Mersenne (1588–1648, France)

- Moine de l'ordre des Minimes. Le nom de l'ordre vient du fait que les Minimes se considéraient comme les plus humbles des religieux ; ils se consacraient à la prière et aux études.

- Mersenne est surtout connu pour son rôle d'intermédiaire entre les savants de son époque ; il faut se rappeler qu'il n'y avait alors ni journaux scientifiques, ni colloques, ni… courriel ! Partisan d'un travail scientifique collectif, il favorisa les échanges entre tous les savants de son temps, leur rendant visite et entretenant avec eux une correspondance abondante et suivie. Il organisa en 1635 l'*Academia Parisiensis*, lieu de rencontre entre savants.[1] À sa mort, on trouva dans sa cellule des lettres de plus de 75 correspondants différents, dont Descartes, Pascal, Fermat, Huygens, Pell, Galilée, Roberval et Torricelli.

1. Outre des regroupements de savants tel celui lancé par Mersenne, les académies scientifiques firent leur apparition en Europe au cours du XVII^e siècle. Certaines d'entre elles devinrent des institutions de toute première importance et, dans plusieurs cas, sont encore actives aujourd'hui. La plus ancienne est l'*Accademia nazionale dei Lincei* (Académie nationale des Lynx), fondée à Rome en 1603 et dont Galilée fut l'un des premiers membres, en 1611. La *Royal Society* (« Royal Society of London for Improving Natural Knowledge ») fut officiellement établie en 1660 — mais des rencontres régulières de savants se tenaient cependant à Londres depuis plus de quinze ans — et compta parmi ses premiers présidents Newton, de 1703 jusqu'à sa mort en 1727. Du côté de la France, c'est en 1666, à l'époque de Louis XIV et à l'instigation de Colbert, que fut créée une première *Académie des sciences*. En 1699, elle fut officiellement placée « sous la protection » du roi et devint l'« Académie royale des sciences » (elle perdit son épithète à la Révolution française). Roberval figure parmi ses membres fondateurs. De nombreuses autres académies européennes furent par la suite mises en place (Berlin, Saint-Pétersbourg, etc.) par des souverains soucieux de soutenir tant les sciences que… leur propre gloire. La plupart des grands mathématiciens européens firent partie au fil des ans de l'une ou l'autre de ces académies. Parmi les mathématiciens français présentement membres de l'Académie des sciences se retrouvent, outre des sommités telles Jean-Pierre Kahane (qui s'est vu décerner un doctorat *honoris causa* de l'Université Laval en 1992) ou Jean-Pierre Serre — tous deux sont nés en 1926 —, de récents médaillés Fields tels Wendelin Werner, né en 1968, et Cédric Villani, né en 1973.

- L'un des premiers savants de laboratoire possédant un « cabinet de physique », Mersenne participa à l'institution de la physique quantitative. Fortement opposé à l'alchimie, à l'astrologie et aux sciences mystiques, il défendit le rationalisme de Descartes et les théories de Galilée, qu'il contribua à faire connaître en dehors de l'Italie. Il proposa à Huygens l'utilisation du pendule pour mesurer le temps, inspirant ainsi les premières horloges à pendule. Ses travaux les plus importants en physique concernent l'acoustique. Il utilisa le phénomène de l'écho pour mesurer la vitesse du son.

- En mathématiques, on lui doit de nombreuses traductions des mathématiciens grecs. Mais c'est surtout en théorie des nombres qu'il a laissé sa marque. Il s'est intéressé aux nombres premiers et a tenté de trouver une formule représentant tous les nombres premiers. Quoiqu'il ait échoué dans ses tentatives, ses travaux sur les nombres premiers de la forme $2^n - 1$ ont trouvé des échos jusqu'à aujourd'hui.

  On appelle *nombre de Mersenne* un nombre de la forme $M_n = 2^n - 1$; si ce nombre est premier, on dit alors que c'est un *premier de Mersenne*. Il est facile de vérifier que si M_n est premier, alors n lui-même doit être premier [2] ; la réciproque est cependant fausse (ainsi, $M_{11} = 2047 = 23 \times 89$). En 1644, Mersenne avait annoncé que $2^n - 1$ est premier si $n = 2$, 3, 5, 7, 13, 17, 19, 31, 67, 127 et 257, mais composé pour les autres 44 nombres premiers inférieurs à 257 ; on sait aujourd'hui qu'il s'est trompé pour cinq de ces nombres : $2^{67} - 1$ et $2^{257} - 1$ sont composés, alors qu'il avait oublié $2^{61} - 1$, $2^{89} - 1$ et $2^{107} - 1$, qui sont premiers. [3] On connaît à ce jour 48 nombres premiers de Mersenne ; le plus grand a été découvert en janvier 2013 : $2^{57\,885\,161} - 1$, un nombre de 17 425 170 chiffres. [4] On ne sait pas s'il existe une infinité de premiers de Mersenne.

---

2. Cette observation est due à Pierre de Fermat (1601–1665) et figure dans une lettre à Mersenne datée de juin 1640. Pour une démonstration, voir le Théorème 1 plus bas.

3. Il peut être intéressant de rappeler l'anecdote suivante à propos du nombre $M_{67} = 2^{67} - 1$. Le mathématicien français Édouard Lucas (1842–1891) avait montré en 1876 que M_{67} est composé, mettant ainsi le doigt sur la première erreur dans la liste de Mersenne. Mais ses méthodes ne lui permettaient pas de connaître les facteurs de ce nombre. Cette question a été résolue quelques années plus tard par le mathématicien américain Frank Nelson Cole (1861–1926), dans un exposé « sans paroles » demeuré célèbre et présenté en octobre 1903 lors d'un congrès de l'American Mathematical Society (voir F.N. Cole, « On the factoring of large numbers. » *Bull. Amer. Math. Soc.*, 10 (1903), 134–137). Après avoir écrit au tableau $2^{67} - 1 = 147\,573\,952\,589\,676\,412\,927$, Cole a patiemment effectué la multiplication

$$761\,838\,257\,287 \times 193\,707\,721,$$

obtenant ainsi le produit 147 573 952 589 676 412 927, puis il est aller se rasseoir, le tout sans dire un seul mot, rapporte-t-on… Cole aurait indiqué que la recherche des facteurs de M_{67} lui aurait pris « trois années de dimanches ». Cette situation peut être vue comme typique de la différence fondamentale, en termes de complexité, entre *trouver* une solution d'un problème et *vérifier* une solution, nuance qui est au coeur même du célèbre problème ouvert ***P*** *vs* ***NP***.

4. Voir à ce sujet sur la Toile les sites `http://www.mersenne.org/` (*The Great Internet Mersenne Prime Search*) et `http://primes.utm.edu/mersenne/`.

Nombres de Mersenne et nombres parfaits

- On appelle *nombre parfait* un nombre qui est égal à la somme de ses diviseurs propres. [5] Par exemple, 6 est parfait, puisque $6 = 1 + 2 + 3$; de même, 28 est parfait.

- La recherche de nombres premiers de Mersenne est reliée à la recherche de nombres parfaits ; en effet, la proposition 36 du Livre IX des *Éléments* d'Euclide affirme que si le nombre de Mersenne $2^n - 1$ est premier, alors $2^{n-1}(2^n - 1)$ est un nombre parfait. [6]

- René Descartes (1596–1650), dans une lettre à Mersenne en 1638, affirme que tout nombre parfait *pair* est « euclidien », c'est-à-dire de la forme $2^{n-1}(2^n-1)$ avec 2^n-1 est premier. Mais il n'indique pas quel est son raisonnement. On ignore s'il avait vraiment une telle preuve ou s'il n'émettait qu'une conjecture.

- Le mathématicien suisse Leonhard Euler (1707–1783), dans un ouvrage posthume, [7] donne le premier une démonstration de l'observation de Descartes (voir Théorème 3 ci-bas). En combinant les résultats d'Euclide et d'Euler, on a ainsi une caractérisation complète des nombres parfaits pairs (voir Corollaire).

- On ne sait pas s'il existe des nombres parfaits impairs. Mais on a montré que de tels nombres seraient forcément supérieurs à 10^{1500}. [8]

- Les quatre premiers nombres parfaits, 6, 28, 496 et 8128, sont connus depuis l'Antiquité. Ils sont notamment mentionnés dans les travaux de Nicomache de Gérase et de Théon de Smyrne (2e siècle apr. J.-C.).

  Le cinquième nombre parfait, 33 550 336, apparaît dans un codex latin datant de 1456. Les sixième et septième nombres parfaits (8 589 869 056 et 137 438 691 328) sont dus à Cataldi (fin du 16$^{\text{e}}$ siècle), tandis que le huitième est dû à Euler (1772) : 2 305 843 008 139 952 128.

---

5. Cette définition est introduite au Livre VII des *Éléments* d'Euclide : « Un nombre *parfait* est celui qui est égal à ses parties » (sous-entendu : à la somme de ses parties) — voir définition VII.23 dans l'édition (française) de B. Vitrac et VII.22 dans celle (anglaise) de T.L. Heath.

6. Autrement dit, si M_n est premier, alors le M_n–ième nombre triangulaire est parfait. Dans le langage d'Euclide, la proposition IX.36 s'énonce comme suit : *Si, à partir de l'unité, des nombres en quantité quelconque sont consécutivement posés en proportion double jusqu'à ce qu'additionnés, leur total devienne premier, et que ce total, multiplié par le dernier, produise un certain nombre, ce produit sera parfait.* Cette proposition, la toute dernière des trois livres des *Éléments* consacrés à l'arithmétique, est en quelque sorte le point culminant de ce thème chez Euclide, et la démonstration qu'il en donne est particulièrement touffue — surtout si on la compare par exemple à sa démonstration de la proposition IX.20 sur l'infinitude des nombres premiers, qui encore maintenant est utilisée telle quelle (cette dernière démonstration demeure d'ailleurs l'archétype d'une « belle preuve »). Le théorème d'Euclide sur les nombres parfaits est aujourd'hui considéré comme un résultat élémentaire en théorie des nombres et on en trouvera plus bas (Théorème 2) une démonstration moderne — en deux variantes.

7. Le *Tractatus de numerorum doctrina capita sedecim, quæ supersunt* (*Traité sur la doctrine des nombres, composé de seize chapitres*) est un projet de livre sur la théorie des nombres écrit par Euler vraisemblablement après 1756, mais publié seulement en 1849. Ce texte est accessible (en latin) sur le site « The Euler Archive » à l'adresse `http://www.math.dartmouth.edu/~euler/`, document E792. Le théorème d'Euler y fait l'objet des paragraphes 106–108.

8. P. Ochem et M. Rao, Odd perfect numbers are greater than 10^{1500}. *Mathematics of Computation* 81 (2012) 1869–1877.

Vers le début des années 1950, 12 nombres parfaits étaient connus. La découverte de nouveaux nombres parfaits s'est depuis considérablement accélérée grâce à des techniques de plus en plus sophistiquées où l'ordinateur a la part belle. Depuis le milieu des années 1990, les nouveaux nombres parfaits identifiés l'ont été dans le cadre du GIMPS.

Voici la liste des huit premiers nombres parfaits.

6	$=$	$2^1(2^2-1)$	*Antiquité*
28	$=$	$2^2(2^3-1)$	*Antiquité*
496	$=$	$2^4(2^5-1)$	*Antiquité*
$8\,128$	$=$	$2^6(2^7-1)$	*Antiquité*
$33\,550\,336$	$=$	$2^{12}(2^{13}-1)$	*Anonyme, 1456*
$8\,589\,869\,056$	$=$	$2^{16}(2^{17}-1)$	*Cataldi, 1588*
$137\,438\,691\,328$	$=$	$2^{18}(2^{19}-1)$	*Cataldi, 1588*
$2\,305\,843\,008\,139\,952\,128$	$=$	$2^{30}(2^{31}-1)$	*Euler, 1772*

Preuves des théorèmes

Théorème 1 (Fermat, 1640)
Soit $M_n = 2^n - 1$; si M_n est premier, alors n est premier.

Démonstration : Afin d'établir que lorsque $2^n - 1$ est premier, n est lui-même forcément premier, nous démontrons plutôt l'affirmation contraposée : si n est composé, alors $2^n - 1$ est aussi composé.

Soit donc $n = ab$, avec $a, b > 1$, et considérons l'identité $x^k - 1 = (x-1)(x^{k-1} + x^{k-2} + \cdots + x + 1)$ dans laquelle nous posons $x = 2^a$ et $k = b$. Il suit alors

$$2^{ab} - 1 = (2^a - 1)(2^{a(b-1)} + 2^{a(b-2)} + \cdots + 2^a + 1),$$

ce qui montre que $2^n - 1 = 2^{ab} - 1$ est composé, puisque factorisé sous forme de deux facteurs chacun supérieur à 1 (car $a > 1$). ■

Théorème 2 (Euclide, IX.36)
Si M_n est premier, alors $2^{n-1}M_n$ est un nombre parfait.

Démonstration 1 : Nous donnons une première démonstration utilisant la fonction $\sigma(n)$ définie comme la somme de tous les diviseurs de l'entier positif n.[9] (Un nombre parfait k est donc caractérisé par le fait que $\sigma(k) = 2k$.)

9. Comme de nombreux outils en théorie des nombres, la fonction $\sigma(n)$ a été introduite par Euler, dans son *Tractatus de numerorum doctrina capita sedecim, quæ supersunt*. Il la dénote alors par le symbole $\int n$. On a par exemple $\sigma(15) = 1 + 3 + 5 + 15 = 24$. À noter que p est premier si et seulement si $\sigma(p) = p + 1$.

On peut se convaincre sans trop de difficulté que la fonction σ possède la propriété suivante : si a et b sont deux naturels *premiers entre eux*, c'est-à-dire tels que $\text{PGCD}(a,b) = 1$, alors $\sigma(ab) = \sigma(a)\sigma(b)$.[10] Dans le cas qui nous intéresse, notons de plus les deux faits suivants :

- comme M_n est premier, on a $\sigma(M_n) = 1 + M_n = 1 + (2^n - 1) = 2^n$;
- $\sigma(2^{n-1}) = 1 + 2 + 2^2 + 2^3 + \cdots + 2^{n-1} = 2^n - 1 = M_n$.

On en tire alors

$$\sigma(2^{n-1}M_n) = \sigma(2^{n-1})\sigma(M_n) = M_n 2^n = 2(2^{n-1}M_n),$$

ce qu'il fallait démontrer. ■

Démonstration 2 : Voici une deuxième démonstration du Théorème 2, dans laquelle on examine directement les diviseurs du nombre $2^{n-1}M_n$.

Posant, pour simplifier la notation, $p = M_n = 2^n - 1$, il nous faut donc montrer que la somme S des diviseurs propres de $2^{n-1}p$ est justement le nombre $2^{n-1}p$ lui-même. Or quels sont les diviseurs propres de $2^{n-1}p$? Comme p est premier, ce sont précisément les $2n - 1$ nombres

$$1, 2, 2^2, \ldots, 2^{n-1}, p, 2p, 2^2p, \ldots, 2^{n-2}p.$$

Il s'agit donc d'évaluer la somme

$$(*) \qquad S = 1 + 2 + 2^2 + \cdots + 2^{n-1} + p + 2p + 2^2p + \cdots + 2^{n-2}p.$$

Notons que les n premiers termes de cette somme forment une progression géométrique, de

10. En théorie des nombres, une fonction ayant cette propriété est appelée *fonction multiplicative* — la fonction $\sigma(n)$ fait partie d'un lot de quelques fonctions « arithmétiques » (i.e. définies sur l'ensemble $\mathbb{N}$ des naturels) intervenant abondamment dans ce champ des mathématiques. La multiplicativité de la fonction $\sigma(n)$ est souvent présentée dans des bouquins de théorie des nombres comme un corollaire de résultats généraux de base sur les fonctions multiplicatives. Mais on peut établir cette propriété directement comme suit. Étant donné a et b tels que $\text{PGCD}(a,b) = 1$, on se convainc facilement que tout diviseur de ab s'écrit de manière unique comme un produit de la forme de, où $d \mid a$ et $e \mid b$ (regardez les factorisations premières de a et de b). Si on appelle $d_1, d_2, \ldots, d_s$ les diviseurs de a et $e_1, e_2, \ldots, e_t$ ceux de b, on a alors

$$\begin{aligned}
\sigma(a)\sigma(b) &= (d_1 + d_2 + \cdots + d_s)(e_1 + e_2 + \cdots + e_t) \\
&= \quad d_1e_1 + d_1e_2 + \cdots + d_1e_t \\
&\quad + d_2e_1 + d_2e_2 + \cdots + d_2e_t \\
&\qquad\qquad \vdots \\
&\quad + d_se_1 + d_se_2 + \cdots + d_se_t.
\end{aligned}$$

Or les termes de cette somme coïncidant avec les diviseurs de ab, celle-ci est donc égale à $\sigma(ab)$, montrant ainsi que $\sigma(ab) = \sigma(a)\sigma(b)$ pour a et b premiers entre eux, et donc que σ est multiplicative.

sorte que $1+2+2^2+\cdots+2^{n-1}=2^n-1=p$. Il s'ensuit un « télescopage » de la somme S :

$$\begin{array}{rcccccccccccc}
S & = & p & + & p & + & 2p & + & 2^2p & + & 2^3p & + & \cdots & + & 2^{n-2}p \\
 & & & = & 2p & + & 2p & + & 2^2p & + & 2^3p & + & \cdots & + & 2^{n-2}p \\
 & & & & & = & 2^2p & + & 2^2p & + & 2^3p & + & \cdots & + & 2^{n-2}p \\
 & & & & & & & = & 2^3p & + & 2^3p & + & \cdots & + & 2^{n-2}p \\
 & & & & & & & & & & & & \vdots & & \\
 & & & & & & & & & & & = & 2^{n-2}p & + & 2^{n-2}p \\
 & & & & & & & & & & & & & = & 2^{n-1}p,
\end{array}$$

ce qu'il fallait démontrer. (On observera que les $n-1$ derniers termes de $(*)$ forment aussi une progression géométrique, ce qui fournirait une autre manière de conclure le raisonnement.) ■

Théorème 3 (Euler, 1849 — publication posthume)
Soit k, un nombre parfait pair. Alors il existe $n \in \mathbb{N}$ tel que $k = 2^{n-1}(2^n-1)$ et $M_n = 2^n-1$ est un nombre premier.

Avant de prouver ce résultat, tirons immédiatement la conséquence suivante des Théorèmes 2 et 3 :

Corollaire (Euclide–Euler)
Soit k, un nombre pair. Alors k est parfait si, et seulement si, k est de la forme

$$k = 2^{n-1}(2^n-1),$$

avec 2^n-1 un nombre premier.

Démonstration : Le « si » ($\Leftarrow$) est le résultat d'Euclide, IX.36, tandis que le « seulement si » ($\Rightarrow$) est dû à Euler. ■

Nous allons donner deux démonstrations du Théorème 3, la première utilisant à nouveau la propriété de multiplicativité de la fonction σ. C'est essentiellement la démonstration donnée par Euler dans son *Tractatus*.

Démonstration 1 : k étant un nombre pair, écrivons-le sous la forme $k = 2^a \cdot b$, où b est un nombre impair et $a > 0$. Comme on a alors $\text{PGCD}(2^a, b) = 1$, on a donc, par multiplicativité de σ,

$$\sigma(k) = \sigma(2^a)\sigma(b) = (2^{a+1}-1)\sigma(b). \tag{1}$$

Tout ce que l'on sait de b étant le fait qu'il est impair, on ne peut rien dire pour le moment à propos de $\sigma(b)$. Mais comme k est parfait, on a

$$\sigma(k) = 2k = 2 \cdot 2^a b = 2^{a+1}b. \tag{2}$$

En combinant les égalités (1) et (2) et en divisant par $(2^{a+1}-1)b$, on obtient

$$\frac{\sigma(b)}{b} = \frac{2^{a+1}}{2^{a+1}-1}. \tag{3}$$

Or le membre de droite de cette dernière égalité est une fraction dont le numérateur surpasse de 1 le dénominateur : il s'agit donc d'une fraction irréductible. Posant alors $c = \text{PGCD}(b, \sigma(b))$, on sait qu'en divisant la fraction de gauche de l'égalité (3) par c, on obtient la fraction à la droite. On a ainsi

$$b = c(2^{a+1} - 1) = c \cdot 2^{a+1} - c, \tag{4}$$

et

$$\sigma(b) = c \cdot 2^{a+1}. \tag{5}$$

Il suit donc de (4) et (5) que

$$\sigma(b) = b + c. \tag{6}$$

Par définition de c, on sait qu'il s'agit d'un naturel ≥ 1. Mais comme $a \geq 1$, on a $2^{a+1} - 1 > 1$, de sorte que c est un diviseur de b autre que b lui-même (par (4)). Or si c était > 1, on aurait, selon la définition même de la fonction σ, que $\sigma(b) \geq b + c + 1$ — on sait en effet que b a au moins ces trois termes comme diviseurs —, contredisant ainsi (6). On en conclut alors que $c = 1$, ce qui monte que le membre de gauche de (3) est lui aussi irréductible.

Posant alors $c = 1$ dans (6), on en tire que $\sigma(b) = b + 1$, ce qui revient au fait que b est un nombre premier. Par ailleurs, la ligne (4) entraîne que $b = 2^{a+1} - 1$. Posant enfin $n = a + 1$, on a que $k = 2^a b = 2^{n-1}(2^n - 1)$, avec $2^n - 1$ un nombre premier, terminant ainsi la démonstration du Théorème 3. ■

Voici une autre démonstration un peu plus « pédestre » du Théorème 3 qui n'utilise pas la propriété de multiplicativité de la fonction σ — cette fonction ne sert alors que de simple notation — et dans laquelle sont rendus explicites certains renseignements que σ recèle. On y voit bien comment se comportent les diviseurs du nombres k.

DÉMONSTRATION 2 : Soit a, l'exposant de la plus grande puissance de 2 que contient k ; on peut donc écrire k sous la forme

$$k = 2^a \cdot b \tag{7}$$

avec $a \geq 1$ (car k est pair, par hypothèse) et b est impair. Afin de simplifier la notation, posons $S = \sigma(b)$, la somme des diviseurs impairs de k.

On partage alors les diviseurs de k en $a + 1$ groupes disjoints, comme suit :

- on considère tout d'abord les diviseurs impairs de k ;
- puis les diviseurs pairs de k tels que, dans leur factorisation première, 2 est affecté de l'exposant 1 ;
- ensuite les diviseurs pairs de k tels que, dans leur factorisation première, 2 est affecté de l'exposant 2 ;
- les diviseurs pairs de k tels que, dans leur factorisation première, 2 est affecté de l'exposant 3 ;

$$\vdots$$

– enfin, les diviseurs pairs de k tels que, dans leur factorisation première, 2 est affecté de l'exposant a.

On a donc [11]

$$\sigma(k) = S + 2^1 \cdot S + 2^2 \cdot S + 2^3 \cdot S + \cdots + 2^a \cdot S.$$

Mais k étant parfait, nous avons $\sigma(k) = 2k$, d'où il suit alors

$$\begin{aligned} 2k &= S + 2 \cdot S + 2^2 \cdot S + 2^3 \cdot S + \cdots + 2^a \cdot S \\ &= S(1 + 2 + 2^2 + 2^3 + \cdots + 2^a) \\ &= S(2^{a+1} - 1). \end{aligned}$$

On en tire que $S = \dfrac{2k}{2^{a+1} - 1}$, c'est-à-dire, en vertu de (7),

$$S = \frac{2^{a+1} \cdot b}{2^{a+1} - 1}. \tag{8}$$

Substituant $\sigma(b)$ à la place de S, on retrouve ainsi l'égalité (3), et la preuve peut alors se poursuivre comme dans la première version. ■

11. Par exemple, le nombre $360 = 2^3 \cdot 3^2 \cdot 5$ est de la forme $2^3 \cdot 45$. On répartit alors les 24 diviseurs de 360 en 4 groupes :

– les diviseurs impairs de 360 (c'est-à-dire les diviseurs de 45) :

1 3 5 9 15 45

dont la somme est 78 ;

– les diviseurs pairs de 360 ayant 2 comme plus grand diviseur pair :

2 6 10 18 30 90

dont la somme est $2 \cdot 78 = 156$;

– les diviseurs pairs de 360 tels que la puissance maximale de 2 qui les divise est 2^2 :

4 12 20 36 60 180

dont la somme est $2^2 \cdot 78 = 312$;

– et enfin les diviseurs pairs de 360 contenant 2^3, la plus grande puissance de 2 possible en l'occurrence :

8 24 40 72 120 360

dont la somme est $2^3 \cdot 78 = 624$.

La somme de tous les diviseurs de 360 est donc $78 + 156 + 312 + 624 = 1170$.