

*Last night I met upon the stair,
A little man who wasn't there.
He wasn't there again today.
I wish to heck he'd go away.*
Anonymous

Les nombres de Mersenne et les nombres parfaits.

Tancrède LEPOINT

Octobre 2008

Table des matières

1	Introduction et début de l'histoire	2
2	Les nombres parfaits et les nombres de Mersenne	4
2.1	Qu'est-ce qu'un nombre parfait?	4
2.2	Relation avec les nombres de Mersenne	4
2.3	La fonction σ	5
3	Le test de Lucas-Lehmer	6
4	Quelques conjectures et problèmes irrésolus	7
4.1	Nombre parfait impair	7
4.2	Infinité de nombre de Mersenne	7
4.3	La nouvelle conjecture de Mersenne	7
4.4	Les nombres doubles de Mersenne	8
5	Pour aller plus loin	8
	Références	8

1 Introduction et début de l'histoire

Dans cette étude, nous allons rechercher les nombres premiers de la forme $a^n - 1$ où $a, n \geq 2$, comme par exemple $31 = 2^5 - 1$. La première constatation évidente est que le nombre a doit être pair. En effet, s'il est impair, a^n est impair et le nombre recherché est pair, donc ne peut être premier (car ≥ 3).

L'autre constatation évidente est que a doit nécessairement être égal à 2. Ceci découle de la formule de la somme des séries géométriques¹ :

$$\begin{aligned}\forall x \in \mathbb{R}, x^n - 1 &= (x - 1) \cdot \sum_{k=0}^{n-1} x^k \\ &= (x - 1) \cdot (1 + x + x^2 + \dots + x^{n-1})\end{aligned}\tag{1}$$

qui est démontrée en développant le terme de droite pour vérifier que l'on obtient bien celui de gauche.

Démonstration. On a donc pour $n \geq 2$, $a^n - 1 = (a - 1) \cdot (1 + a + \dots + a^{n-1})$, et comme on veut que $a^n - 1$ soit premier, ses seuls diviseurs sont 1 et lui-même. D'où $a - 1 = 1$, i.e $a = 2$. \square

En testant les valeurs sur les premiers nombres $n \geq 2$, on a :

$2^2 - 1 = 3$	premier
$2^3 - 1 = 7$	premier
$2^4 - 1 = 15 = 3 \cdot 5$	non premier
$2^5 - 1 = 31$	premier
$2^6 - 1 = 63 = 7 \cdot 9$	non premier
$2^7 - 1 = 127$	premier

Viens alors une première proposition :

Proposition 1. *Si $2^n - 1$ est premier alors n doit être premier*

Démonstration. En effet, si $n = mk$ avec $m \notin \{1, n\}$, alors on peut montrer que $2^n - 1$ est divisible par $2^m - 1$, comme conséquence immédiate de (1) : $2^n - 1 = (2^m)^k - 1 =$

$$\underbrace{(2^m - 1)}_{\neq 1} \cdot \left(\sum_{l=1}^{k-1} (2^m)^l \right) \quad \square$$

Suit alors la première conjecture :

Conjecture 2. Tous les nombres de la forme $2^n - 1$ sont premiers quelque soit l'entier naturel premier n

1. Que tout élève sérieux se doit de savoir parfaitement !

C'est en 1536 que Hudalricus Regius a montré que ce résultat était faux car $2^{11} - 1 = 2047 = 23 \cdot 89$.

Les mathématiciens ont continué leur recherche et après avoir montré en 1603 que $2^{17} - 1$ et $2^{19} - 1$ étaient tous les deux premiers, Pietro Cataldi a émis la conjecture suivante :

Conjecture 3 (Pierre Cataldi). Les nombres de la forme $2^n - 1$ avec $n = 23, 29, 31$ et 37 sont premiers

En 1640, soit 37 ans plus tard, Fermat a montré que Cataldi avait tort pour 23 et 37. Et en 1738, Euler a démontré qu'il avait aussi tort pour $n = 29$, mais raison pour $n = 31$.

Et c'est en 1644, dans la préface de *Cogita Physica-Mathematica* que le moine Marin Mersenne a émis la conjecture (encore fausse!) suivante :

Conjecture 4 (Mersenne). Les nombres de la forme $2^n - 1$ sont premiers pour $n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127$ et 257 et sont composés (i.e. non premiers) pour tous les autres entiers inférieurs à 257.

Bien que la conjecture de Mersenne soit fausse, c'est son nom plutôt que celui de Regius qui a été retenu, et on a donc la définition suivante :

Définition 5. Les nombres de la forme $2^n - 1$ sont appelés **nombres de Mersenne**, et seront notés M_n .

Ce n'est seulement qu'en 1883 (!) que Pervouchine a trouvé que le nombre $2^{61} - 1$ était premier et que la conjecture était fausse puisque 61 n'était pas dans la liste. Sept ans auparavant, Lucas² avait montré qu'effectivement $2^{127} - 1$ était premier. Finalement, une autre erreur a été soulevée, $2^{67} - 1$ n'étant pas premier. Au début du vingtième siècle, Powers a montré que $2^{89} - 1$ et $2^{107} - 1$ étaient aussi premiers (et absents de la liste). Finalement, en 1947 paraissait la liste finale et vérifiée des nombres premiers p inférieurs à 258 tels que $2^p - 1$ soit premier :

$$p = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127$$

Au jour d'aujourd'hui, l'avènement de l'informatique a permis de déterminer 46 nombres de Mersenne, le dernier ayant été découvert en septembre 2008. Il est possible de participer à la recherche du plus gros nombre premier³ en téléchargeant le logiciel de GIMPS⁴ sur le site web :

<http://www.mersenne.org/prime.htm>

2. Lucas a mis au point un test qui permet de tester facilement la primalité des nombres de Mersenne. Nous y reviendrons par la suite

3. Car ils sont obtenus avec les nombres de Mersenne, comme on le verra par la suite

4. Great Internet Mersenne Prime Search

2 Les nombres parfaits et les nombres de Mersenne

2.1 Qu'est-ce qu'un nombre parfait ?

Les mathématiciens grecs ont observé dès l'Antiquité qu'il y avait une relation entre un nombre et la somme de ses diviseurs (ce qui a souvent provoqué des interprétations mystiques⁵). Ici, nous nous intéressons à une de ces relations :

Définition 6. Un entier naturel n est dit **nombre parfait** s'il est égal à la somme de tous ses diviseurs positifs, en excluant n lui-même

Exemples. Le nombre 6 a comme diviseurs positifs 1, 2, 3 et 6 et $6 = 1 + 2 + 3$. De même $28 = 1 + 2 + 4 + 7 + 14$ est aussi un nombre parfait. Les deux suivants sont 496 et 8128, et ils étaient connus avant l'an 1.

2.2 Relation avec les nombres de Mersenne

Si l'on regarde les quatre nombres parfaits précédents sous une forme partiellement

$$\begin{array}{rcll} & 6 & = & 2 \cdot 3 & = & 2 \cdot M_2 \\ \text{factorisée, on observe que :} & 28 & = & 4 \cdot 7 & = & 2^2 \cdot M_3 \\ & 496 & = & 16 \cdot 31 & = & 2^4 \cdot M_5 \\ & 8128 & = & 64 \cdot 127 & = & 2^6 \cdot M_7 \end{array}$$

Etonnement, les nombres de Mersenne semblent intervenir grandement dans les nombres parfaits ! La proposition suivante apparaît comme la proposition 36 du livre IX des *Éléments* d'Euclide :

Proposition 7 (Formule d'Euclide sur les nombres parfaits). *Si $2^p - 1$ est un nombre premier, alors $2^{p-1}(2^p - 1)$ est un nombre parfait.*

Démonstration. Montrons que $2^{p-1}M_p$ est un nombre parfait.

Les diviseurs positifs de ce nombre (celui-ci exclu) sont 1, 2, $2^2, \dots, 2^{p-1}$ et $M_p, 2M_p, 2^2M_p, \dots, 2^{p-2}M_p$. En ajoutant les premiers et en utilisant la somme de série géométrique (1), on a

$$1 + 2 + 2^2 + \dots + 2^{p-1} = \frac{2^p - 1}{2 - 1} = M_p \quad (2)$$

En ajoutant les seconds et en utilisant également la somme de série géométrique (1), on a

$$M_p + 2M_p + 2^2M_p + \dots + 2^{p-2}M_p = M_p \frac{2^{p-1} - 1}{2 - 1} = M_p(2^{p-1} - 1) \quad (3)$$

D'où, en ajoutant (2) et (3), on obtient

$$M_p + M_p(2^{p-1} - 1) = 2^{p-1}(2^p - 1)$$

qui est le nombre de départ, donc parfait ! □

5. Mais le sujet n'est pas là ! Pour plus de renseignement, vous pouvez vous renseigner sur Internet.

On peut ainsi trouver de très grands nombres parfaits. Par exemple, pour $p = 17$, $M_p = 131071$ et $2^{16}(2^{17} - 1) = 8589869056$ est parfait !

Mais ce qui est génial, c'est que la réciproque est vraie (enfin partiellement) ! Environ 2000 ans après Euclide, c'est Leonhard Euler a montré que la formule d'Euclide donnait tous les nombres parfaits *pairs*.

Théorème 8 (Théorème d'Euclide sur les nombres parfaits). *Si n est un nombre parfait pair, alors*

$$n = 2^{p-1}(2^p - 1)$$

où $2^p - 1$ est un nombre de Mersenne premier.

Afin de prouver ce théorème, il va falloir introduire la fonction σ telle que $\sigma(n)$ soit égal à la somme de tous les diviseurs positifs de n (1 et n inclus).

2.3 La fonction σ

Définition 9. Pour tout nombre entier $n \geq 1$, on définit $\sigma(n) = \sum_{d \in \mathbb{N}, d|n} d$

Exemples. – Si p est un nombre premier, $\sigma(p) = p + 1$ (les seuls diviseurs positifs de p sont 1 et lui-même).

– Si $n = p^k$ est une puissance d'un nombre premier p , alors

$$\sigma(n) = \sigma(p^k) = 1 + p + p^2 + \dots + p^k = \frac{p^{k+1} - 1}{p - 1}$$

– Si n est un nombre parfait, alors $\sigma(n) = 2n$

Théorème 10. *Si m et n sont deux entiers premiers entre eux, alors*

$$\sigma(mn) = \sigma(m)\sigma(n) \tag{4}$$

Remarque. De la même manière que l'indicateur d'Euler φ qui vérifie cette même propriété, on peut ainsi calculer $\sigma(n)$ pour de grands n facilement :

$$\begin{aligned} \sigma(16072) &= \sigma(2^3 \cdot 7^2 \cdot 41) \\ &= \sigma(2^3) \cdot \sigma(7^2) \cdot \sigma(41) \\ &= (1 + 2 + 2^2 + 2^3)(1 + 7 + 7^2)(1 + 41) \\ &= 15 \cdot 57 \cdot 42 = 35910 \end{aligned}$$

Démonstration. Si $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k}$, alors

$$\begin{aligned} \sigma(n) &= \sum_{\substack{0 \leq \beta_1 \leq \alpha_1 \\ \dots \\ 0 \leq \beta_k \leq \alpha_k}} p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \dots \cdot p_k^{\beta_k} \\ &= \prod_{i=1}^k (1 + p_i + \dots + p_i^{\alpha_i}) \\ &= \prod_{i=1}^k \left(\frac{p_i^{\alpha_i+1} - 1}{p_i - 1} \right) \end{aligned}$$

Si m et n sont premiers entre eux, alors il n'ont aucun nombre premier en commun dans leur décomposition en nombres premiers. La relation cherchée découle immédiatement de la formule précédente. \square

Remarque. Comme la fonction indicateur d'Euler permet de démontrer rapidement le petit théorème de Fermat, la fonction σ permet de démontrer rapidement la Formule d'Euclide sur les nombres parfaits (Proposition 7) :

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

Cette fonction introduite, nous pouvons maintenant prouver le Théorème d'Euclide sur les nombres parfaits (Théorème 8), que je ne résiste pas au plaisir de vous remettre ci-dessous :

Théorème (Théorème d'Euclide sur les nombres parfaits). *Si n est un nombre parfait pair, alors*

$$n = 2^{p-1}(2^p - 1)$$

où $2^p - 1$ est un nombre de Mersenne premier.

Démonstration. Comme n est pair, il existe un entier $p \geq 2$ tel que $n = 2^{p-1}m$, avec m impair. Comme $m \wedge 2^{p-1} = 1$, on peut utiliser (4), de sorte que $\sigma(n) = \sigma(2^{p-1})\sigma(m) = (2^p - 1)\sigma(m)$. Or n est parfait, donc $\sigma(n) = 2n = 2^p m$. Donc $2^p m = (2^p - 1)\sigma(m)$, d'où $2^p - 1 | 2^p m$. Comme $2^p \wedge 2^p - 1 = 1$, par le lemme de Gauss on a $2^p - 1 | m$, donc il existe l tel que $m = l \cdot (2^p - 1)$. Donc la relation $2^p m = \sigma(n) = (2^p - 1)\sigma(m)$ implique $\sigma(m) = 2^p l = m + l$.

Si $l > 1$, m a au moins 3 diviseurs distincts : $1, l$ et m d'où $\sigma(m) \geq 1 + l + m$, ce qui est absurde. Donc $l = 1$, $m = 2^p - 1$ et $\sigma(m) = m + 1$ donc m est premier. En résumé, $n = 2^{p-1}(2^p - 1)$ et $2^p - 1$ est premier. \square

3 Le test de Lucas-Lehmer

La question est comment trouver les nombres de Mersenne premiers ? Lucas a donné une réponse en proposant un test de primalité d'un nombre de Mersenne, et ce test a été utilisé encore très récemment pour trouver les nombres de Mersenne premiers par ordinateur.

Test (Lucas). Soit p un nombre premier impair. Le nombre de Mersenne $M_p = 2^p - 1$ est premier si, et seulement si, $2^p - 1$ divise $S(p - 1)$ où $S(n + 1) = S(n)^2 - 2$ et $S(1) = 4$.

Démonstration. Devant la difficulté de la preuve, je vous renvoie à l'ouvrage *An Introduction to the Theory of Numbers* de Hardy et Wright, paragraphe 15.5. \square

Exemple. Si l'on prend $p = 7$, $M_p = 127$. Calculons $S(6)$.

$$S(1) = 4$$

$$S(2) = 4^2 - 2 = 14$$

$$S(3) = 14^2 - 2 = 194$$

$$S(4) = 194^2 - 2 = 37634$$

$$S(5) = 37634^2 - 2 = 1416317954$$

$$S(6) = 2005956546822746114 = 127 \cdot 15794933439549182$$

donc M_7 est premier !

L'avantage de ce test (pour les grands nombres, on voit bien que pour $p = 7$ ce n'est pas très pratique), c'est que les ordinateurs fonctionnent en binaire et que la réduction modulo $2^n - 1$ est particulièrement simple. Chaque minute de calcul sur ordinateur correspond à plusieurs années de travail pour quelqu'un utilisant une calculatrice à la main.

4 Quelques conjectures et problèmes irrésolus

4.1 Nombre parfait impair

Existe-t-il un nombre parfait impair ?

En effet, nous savons que tous les nombres parfaits pairs s'écrivent avec les nombres de Mersenne, mais on ne sait même pas si il en existe un seul impair. Néanmoins, on connaît certains résultats sur les éventuels nombres parfaits impairs. On sait que par exemple, s'il en existe un, il a au moins 300 chiffres décimaux, 8 facteurs premiers distincts et son plus grand facteur premier est supérieur à 100110.

4.2 Infinité de nombre de Mersenne

Existe-t-il une infinité de nombre de Mersenne ?, ou, de façon équivalente, **L'ensemble des nombres parfaits pairs est-il infini ?**

4.3 La nouvelle conjecture de Mersenne

Les mathématiciens Bateman, Selfridge et Wagstaff ont conjecturé ce qui suit :

Conjecture 11. Si p est un nombre naturel impair qui vérifie 2 des 3 conditions suivantes, alors il vérifie la troisième :

1. $p = 2^k \pm 1$ ou $p = 4^k \pm 3$
2. $2^p - 1$ est premier (donc un nombre de Mersenne premier !)
3. $\frac{(2^p + 1)}{3}$ est premier.

L'intérêt si cette conjecture est vérifiée est que selon le nombre de p que l'on trouvera vérifiant les axiomes 1. et 3., on pourra déterminer le cardinal des nombres de Mersenne premiers.

4.4 Les nombres doubles de Mersenne

Définition 12. Un nombre double de Mersenne est un nombre de Mersenne de la forme

$$M_{M_p} = 2^{2^p-1} - 1$$

Puisque un nombre de Mersenne M_n peut être premier si et seulement si n est premier, un nombre double de Mersenne M_{M_n} est premier seulement si M_n est premier. Les premières valeurs de n pour lesquelles ceci est vrai sont $n = 2, 3, 5, 7, 13, 17, 19, 31$. De celles-ci, M_{M_n} est connu pour être premier pour $n = 2, 3, 5, 7$; pour $n = 13, 17, 19$, et 31, des facteurs explicites ont été trouvés. Si un autre nombre premier double de Mersenne est un jour trouvé, il serait presque certainement le plus grand nombre premier jamais connu!⁶

5 Pour aller plus loin

Exercice 1 (Un résultat rigolo⁷). Si vous summez les chiffres d'un nombre parfait pair (excepté 6), puis summez les chiffres du nombre résultant, et que vous répétez ce processus jusqu'à obtenir un seul chiffre, ce sera 1.

Hint : Il faut raisonner modulo 9.

Exemple. $8128 \Rightarrow 8 + 1 + 2 + 8 = 19 \Rightarrow 1 + 9 = 10 \Rightarrow 1 + 0 = 1!$

Exercice 2 (Les nombres de Fermat). Soit $n \in \mathbb{N}^*$.

i) Si $2^n + 1$ est premier, montrer que n est une puissance de 2.

Notons maintenant $F_k = 2^{2^k} + 1$. Fermat pensait que tous les F_k étaient premiers, mais Euler a montré en 1732 que $F_5 = 641 \cdot 6700417$. Les nombres premiers de la forme F_k sont appelés les nombres premiers de Fermat.

ii) Montrer que si $k \neq m$, les nombres F_k et F_m sont premiers entre eux. (*Hint : si $k > m$, montrer que F_m divise $F_k - 2$*).

Exercice 3 (Critère de factorisabilité des nombres de Mersenne⁸). Si $k > 1$ et $p = 4k + 3$ est premier, alors une condition nécessaire et suffisante pour que $2^p + 1$ soit premier est que

$$2^p \equiv 1 \pmod{2p + 1}$$

Ainsi, si $2p + 1$ est premier, $(2p + 1) | M_p$ et M_p est composé.

6. Si vous voulez vous renseigner, et/ou vous joindre à Tony Forbes pour connaître la primalité du terme suivant $M_{M_{61}}$, vous pouvez visiter le site web suivant : <http://anthony.d.forbes.googlepages.com/mm61.htm>

7. Vous trouverez la démonstration sur le site Internet : <http://primes.utm.edu/mersenne/index.html>

8. Vous trouverez la démonstration soit dans le Gourdon *Algèbre*, soit dans l'excellent ouvrage de Hardy et Wright : *An Introduction to the Theory of Numbers*.

Références

- [1] Joseph H. Silverman, *A friendly introduction to Number Theory*, - Third edition -
- [2] Hardy and Wright, *An Introduction to the Theory of Numbers*, - Fourth edition -, 1968
- [3] Xavier Gourdon, *Les maths en tête - Algèbre*, Ellipses, 1994
- [4] [http ://primes.utm.edu/mersenne/index.html](http://primes.utm.edu/mersenne/index.html)