Fermat et la factorisation des entiers

par « blogdemaths »
(auteur sous pseudonyme)

Pierre de Fermat était un mathématicien très habile avec les nombres et il savait facilement effectuer des calculs opératoires avec des entiers à dix ou douze chiffres. Cette maîtrise technique s'accompagnait de beaucoup d'astuce et d'ingéniosité de sa part. Nous savons cela aujourd'hui grâce aux nombreuses correspondances qu'il a eues avec ses contemporains.

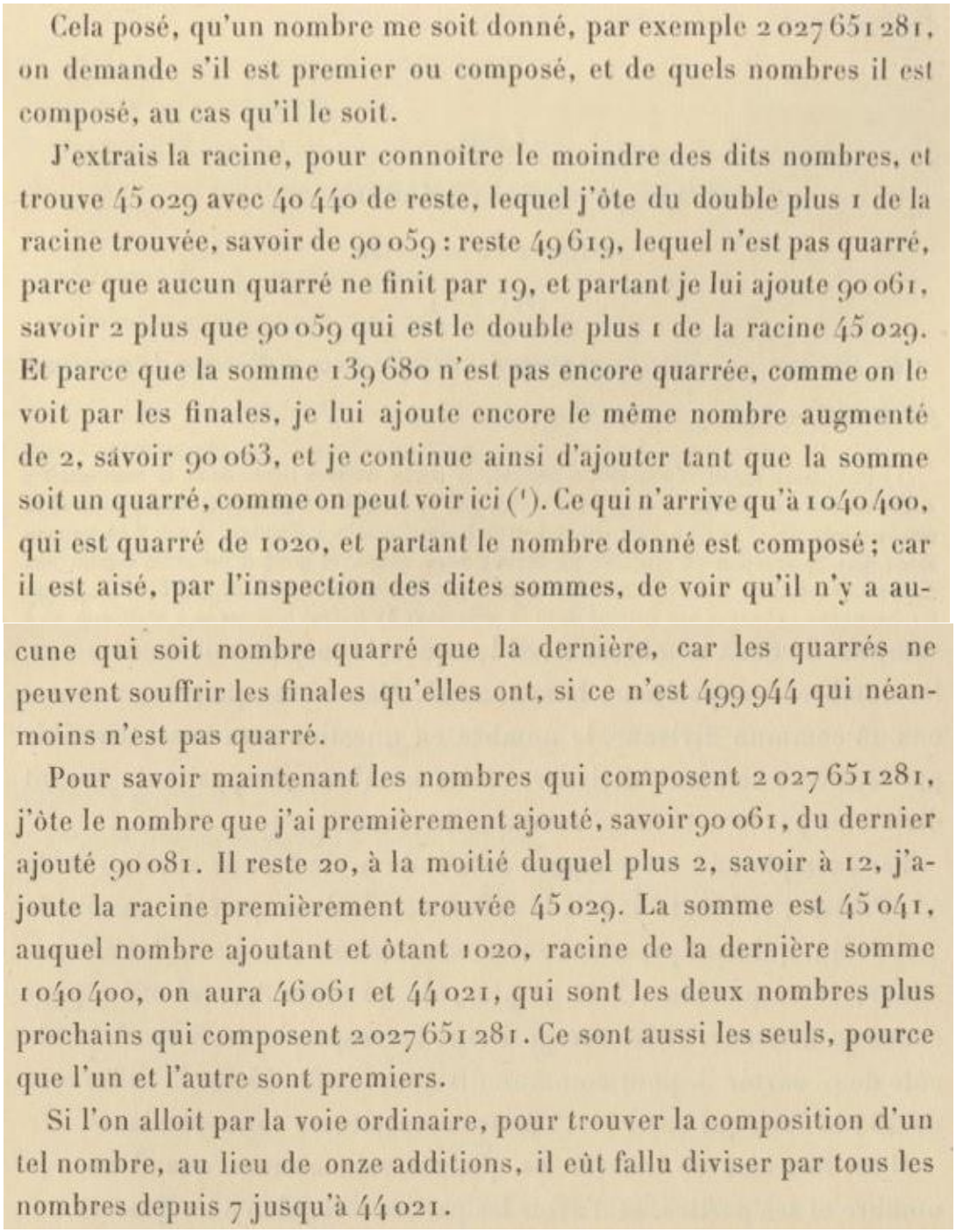
Pour bien se rendre compte des talents arithmétiques de Fermat, voici l'étude de deux de ses lettres, chacune datant de 1643, dans lesquelles il factorise des entiers à 10 et 12 chiffres.

Figure 1 : Pierre de Fermat (ca 1601-1665) *(gravure de François Poilly, 1623-1693).*

1. La méthode de factorisation de Fermat - Fragment d'une lettre de 1643

La question de savoir factoriser un nombre entier est cruciale de nos jours : de nombreux systèmes cryptographiques (dont le fameux RSA) reposent sur cela. Mais, au XVII^{e} siècle, du temps de Fermat, savoir factoriser un entier n'avait absolument aucune application pratique ; le seul intérêt de trouver une factorisation était éventuellement ludique.

Fermat avait trouvé une méthode de factorisation qu'il exposa dans une lettre datée de 1643, dont voici un extrait :



Cela posé, qu'un nombre me soit donné, par exemple 2 027 651 281, on demande s'il est premier ou composé, et de quels nombres il est composé, au cas qu'il le soit.

J'extrais la racine, pour connoître le moindre des dits nombres, et trouve 45 029 avec 40 440 de reste, lequel j'ôte du double plus 1 de la racine trouvée, savoir de 90 059 : reste 49 619, lequel n'est pas quarré, parce que aucun quarré ne finit par 19, et partant je lui ajoute 90 061, savoir 2 plus que 90 059 qui est le double plus 1 de la racine 45 029. Et parce que la somme 139 680 n'est pas encore quarrée, comme on le voit par les finales, je lui ajoute encore le même nombre augmenté de 2, savoir 90 063, et je continue ainsi d'ajouter tant que la somme soit un quarré, comme on peut voir ici (1). Ce qui n'arrive qu'à 1 040 400, qui est quarré de 1020, et partant le nombre donné est composé ; car il est aisé, par l'inspection des dites sommes, de voir qu'il n'y a aucune qui soit nombre quarré que la dernière, car les quarrés ne peuvent souffrir les finales qu'elles ont, si ce n'est 499 944 qui néanmoins n'est pas quarré.

Pour savoir maintenant les nombres qui composent 2 027 651 281, j'ôte le nombre que j'ai premièrement ajouté, savoir 90 061, du dernier ajouté 90 081. Il reste 20, à la moitié duquel plus 2, savoir à 12, j'ajoute la racine premièrement trouvée 45 029. La somme est 45 041, auquel nombre ajoutant et ôtant 1020, racine de la dernière somme 1 040 400, on aura 46 061 et 44 021, qui sont les deux nombres plus prochains qui composent 2 027 651 281. Ce sont aussi les seuls, pource que l'un et l'autre sont premiers.

Si l'on alloit par la voie ordinaire, pour trouver la composition d'un tel nombre, au lieu de onze additions, il eût fallu diviser par tous les nombres depuis 7 jusqu'à 44 021.

Comme on le constate, Fermat expose sa méthode sans réelle explication, ni justification. Nous allons donc détailler cette méthode, et cela, à l'aide d'un formalisme plus contemporain.

1.1 Une idée simple mais brillante

Soit N un entier naturel qu'on veut factoriser. La méthode de Fermat découle de l'idée toute simple suivante : si on peut écrire N comme une différence de deux carrés $N = a^2 - b^2$, alors $N = (a - b)(a + b)$. Le problème de la factorisation se ramène donc à un problème de soustraction. Par exemple, $15 = 4^2 - 1^2 = (4 - 1)(4 + 1) = 3 \times 5$.

Remarquons que si N est un nombre impair, une telle factorisation existe toujours. En effet, si $N = 2n + 1$ alors vous pouvez vérifier que $N = (n+1)^2 - n^2$. Il faut faire tout de même attention car dans ce cas nous avons $a = n + 1$ et $b = n$, ce qui donne $a - b = 1$ et $a + b = 2n + 1 = N$: la factorisation obtenue est donc triviale (savoir que $N = N \times 1$ n'a aucun intérêt, vous en conviendrez).

1.2 Deux conditions nécessaires

Dans toute la suite, on supposera que N n'est pas un carré (car sinon, la factorisation de N est facile à trouver: c'est $N = \sqrt{N} \times \sqrt{N}$). Si on est capable de trouver une décomposition en une différence de deux carrés, autrement dit si $N = a^2 - b^2$ alors,

1. $a^2 - N$ est un carré
2. $a \geq E(\sqrt{N}) + 1$ où $E(\sqrt{N})$ est la partie entière de $\sqrt{N}$.

Explication : Le 1. est évident. Pour le 2., il faut remarquer que $a^2 = N + b^2 > N$ (strict car N n'est pas un carré) et donc $a > \sqrt{N}$, ce qui implique $a \geq E(\sqrt{N}) + 1$.

1.3 Principe général de la méthode de Fermat

On note toujours N le nombre à factoriser et on pose $q = E(\sqrt{N})$. Puisque l'idée est de trouver a et b tels que $N = a^2 - b^2$ et puisqu'on a vu (*cf*. le paragraphe précédent sur les conditions nécessaires) que si a existe alors $a \geq q + 1$, alors on va choisir successivement $a = q + 1$, $a = q + 2$, $a = q + 3$, ...

jusqu'à ce qu'il y ait un a tel que $a^2 - N$ soit un carré. Facile, non ? Voici un exemple simple pour illustrer cette méthode : supposons qu'on souhaite factoriser $N = 799$. On a $\sqrt{799} \approx 28{,}2\ldots$ donc $q = 28$.

1. On essaye avec $a = q + 1 = 29$. On a $a^2 - N = 29^2 - 799 = 43$. Ce n'est pas un carré.
2. On essaye avec $a = q + 2 = 30$. On a $a^2 - N = 30^2 - 799 = 101$. Ce n'est pas un carré.
3. On essaye avec $a = q + 3 = 31$. On a $a^2 - N = 31^2 - 799 = 162$. Ce n'est pas un carré.
4. On essaye avec $a = q + 4 = 32$. On a $a^2 - N = 32^2 - 799 = 225$. C'est un carré !

Comme $225 = 15^2$, on pose $b = 15$, et on a donc la relation $a^2 - N = b^2$. Ainsi,

$$N = a^2 - b^2 = 32^2 - 15^2 = (32 + 15)(32 - 15)$$

et on en déduit que $N = 47 \times 17$.

1.4 Raffinement

Dans le cas où le nombre N est très grand, le nombre d'étapes et de calculs est potentiellement très élevé. Pour que cette méthode soit utilisable d'un point de vue pratique, il va falloir minimiser le nombre de calculs, et pour cela, nous allons essayer de voir comment réutiliser les calculs déjà effectués au fur et à mesure. En particulier, il va être possible de calculer les $a^2 - N$ facilement.

Puisqu'on pose successivement $a = q + 1$, $a = q + 2$, etc. nous allons donc utiliser la notation $a_k = q + k$. Essayons de trouver une relation de récurrence:

$$a_{k+1}^2 - N = ((q + k) + 1)^2 - N = (q + k)^2 + 2(q + k) + 1 - N$$

En réarrangeant les termes, on a :

$$a_{k+1}^2 - N = (q + k)^2 - N + 2(q + k) + 1$$

Nous voyons donc que:

$$\boxed{a_{k+1}^2 - N = a_k^2 - N + 2a_k + 1}$$

Il reste maintenant à voir sur un exemple pratique comment utiliser cette relation de récurrence pour exécuter la méthode de Fermat.

1.5 Analyse de l'exemple donné par Fermat dans sa lettre

Dans sa lettre, Fermat décrit en pratique sa méthode pour factoriser le nombre $N = 2027651281$. En posant $q = E(\sqrt{N}) = 45029$, voici ce que cette méthode donne sous forme de tableau:

k	a	$2a+1$	$a^2 - N$
1	45030	90061	49619
2	45031	90063	139680
3	45032	90065	229743
4	45033	90067	319808
5	45034	90069	409875
6	45035	90071	499944
7	45036	90073	590015
8	45037	90075	680088
9	45038	90077	770163
10	45039	90079	860240
11	45040	90081	950319
12	45041	90083	1040400

Vous voyez que ce tableau est très facile à remplir car:

1. a augmente de 1 à chaque fois
2. $2a+1$ augmente de 2 à chaque fois
3. $a^2 - N$ s'obtient en faisant la somme des deux cases situées au-dessus (à la manière du triangle de Pascal) et cela vient de la relation de récurrence que nous avons démontrée au paragraphe précédent. Il n'y a donc

aucune multiplication à faire, ni aucun carré à calculer ! (à part pour la première ligne bien sûr – c'est-à-dire le calcul de $a_1^2 - N$).

Dans l'exemple ci-dessus, on s'est arrêté dès qu'on est tombé sur un carré dans la dernière colonne: en effet, on a $1040400 = 1020^2$ et donc, comme énoncé par Fermat dans son texte, on a

$$N = 45\ 041^2 - 1020^2 = (45\ 041 + 1020)(45\ 041 - 1020) = 46\ 061 \times 44\ 021$$

Comme vous l'avez sans doute constaté dans la lettre, Fermat savait directement reconnaître un nombre qui n'est pas un carré, s'épargnant ainsi un calcul de racine carrée. Il utilisait la condition nécessaire suivante: si un nombre est un carré alors ses deux derniers chiffres sont 00, 01, 04, 09, 16, 21, 24, 25, 29, 36, 41, 44, 49, 56, 61, 64, 69, 76, 81, 84, 89, ou 96 (mais attention, ce n'est pas une condition suffisante). Dans l'exemple ci-dessus, vous voyez immédiatement que les seuls nombres qui peuvent potentiellement être des carrés dans la dernière colonne sont 499 944 et 1 040 400.

2. La factorisation de 100 895 598 169 - Lettre du 7 Avril 1643

Dans une lettre envoyée à Fermat en 1643, le père Mersenne[1] (prêtre qui a donné son nom aux fameux nombres de Mersenne) demanda à Fermat de factoriser le nombre 100 895 598 169. Il reçut aussitôt une lettre de Fermat (datée du 7 avril 1643) dans laquelle on pouvait lire ceci[2] :

> *Vous me demandez si le nombre 100 895 598 169 est premier ou non, et une méthode pour découvrir, dans l'espace d'un jour, s'il est premier ou composé. À cette question, je réponds que ce nombre est composé et se fait du produit de ces deux : 898 423 et 112 303, qui sont premiers.*

Sans calculatrice et en moins d'un jour, Fermat a réussi à factoriser un nombre à 12 chiffres ! Impressionnant ! Mais comment Fermat a-t-il fait pour factoriser ce nombre ? Car malheureusement il n'a pas décrit sa méthode dans cette lettre... (c'était une habitude il faut croire !)

1. Voir des extraits de *Questions Inouyes*… (1634) de Mersenne, en ligne et analysées par S. Taussig sur BibNum (février 2010).
2. Nous simplifions ici le texte de la lettre, dont on trouvera l'extrait réel plus bas.

Figure 2 : Le père Marin Mersenne (1588-1648) *(WikiCommons, portrait s.d.)*

2.1 Échec de la précédente méthode de Fermat

Tout d'abord, il est peu probable que Fermat ait utilisé la méthode de factorisation que nous avons décrite précédemment. En effet, lorsqu'on programme cette méthode sur un ordinateur pour factoriser $N = 100895598169$, on trouve qu'il faudrait $k = 187723$ étapes avant que l'algorithme ne se termine ! Et on a alors

$$a^2 - N = (q+k)^2 - N = (317640 + 187723)^2 - 100895598169 = 154496163600$$

qui est le carré de $b = 393060$. Ainsi, on a :

$$N = (a+b)(a-b) = (q+k+b)(q+k-b)$$

et donc

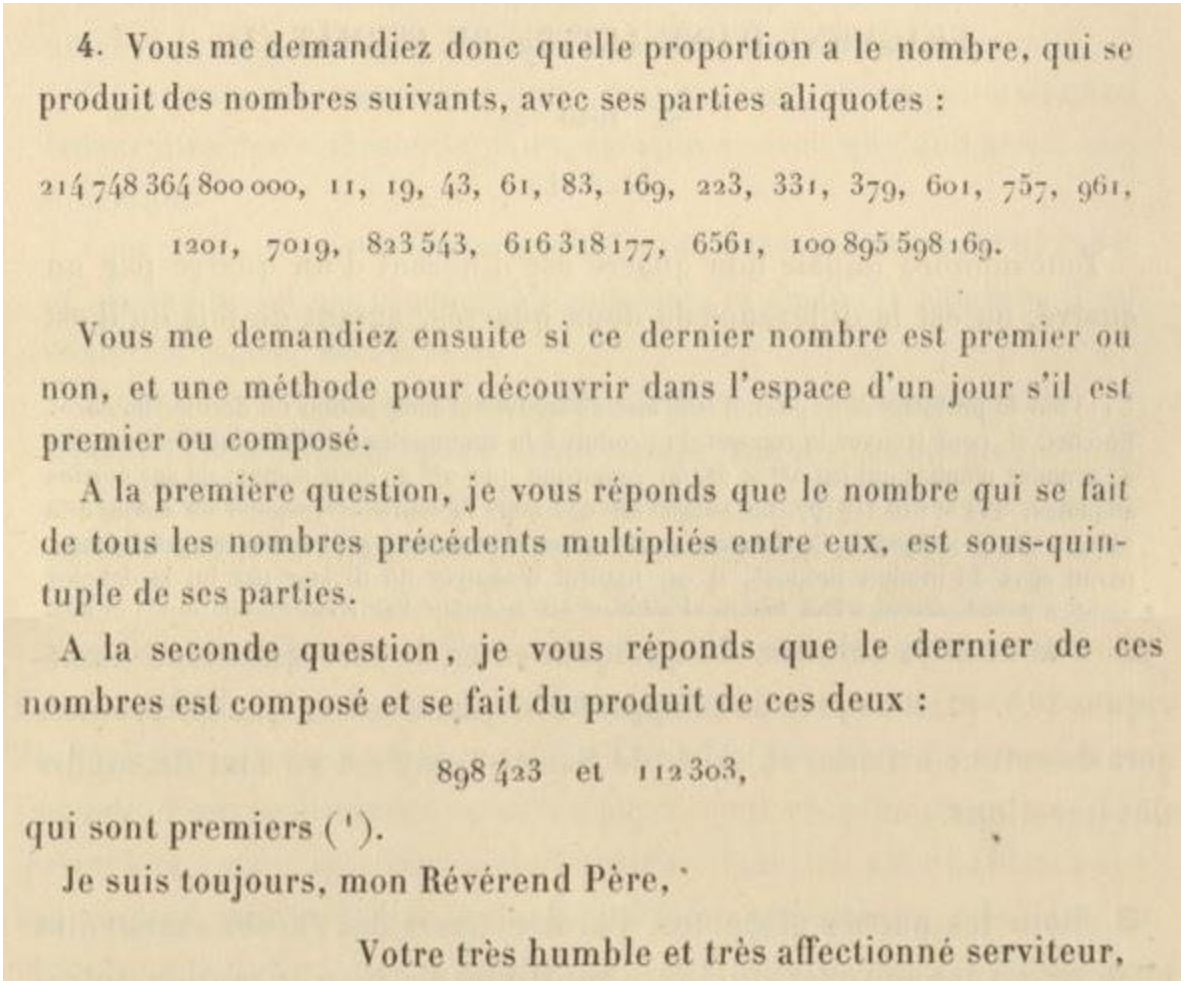
$$N = (317640 + 187723 + 393060) \times (317640 + 187723 - 392060)$$

c'est-à-dire $N = 898423 \times 112303$. On retrouve bien la réponse donnée par Fermat à Mersenne mais il est difficile d'imaginer que Fermat a effectué à la main le calcul de ces 187 723 étapes… La méthode qu'il a utilisée ici est plus astucieuse et s'appuie sur la nature même du nombre 100895598169, qui n'a

pas été proposé par hasard par Mersenne. Pour comprendre le raisonnement de Fermat, commençons par donner un plus grand extrait de sa correspondance.

2.2 Quelques éclaircissements sur cette lettre

Voici donc l'extrait plus large de cette lettre datant du 7 avril 1643 :



4. Vous me demandiez donc quelle proportion a le nombre, qui se produit des nombres suivants, avec ses parties aliquotes :

214 748 364 800 000, 11, 19, 43, 61, 83, 169, 223, 331, 379, 601, 757, 961, 1201, 7019, 823 543, 616 318 177, 6561, 100 895 598 169.

Vous me demandiez ensuite si ce dernier nombre est premier ou non, et une méthode pour découvrir dans l'espace d'un jour s'il est premier ou composé.

A la première question, je vous réponds que le nombre qui se fait de tous les nombres précédents multipliés entre eux, est sous-quintuple de ses parties.

A la seconde question, je vous réponds que le dernier de ces nombres est composé et se fait du produit de ces deux :

898 423 et 112 303,

qui sont premiers (1).

Je suis toujours, mon Révérend Père,

Votre très humble et très affectionné serviteur,

Dans cet lettre, Fermat affirme que le nombre:

$$N = 214748364800000 \times 11 \times 19 \times 43 \times 61 \times 83 \times 169$$
$$\times 223 \times 331 \times 379 \times 601 \times 757 \times 961 \times 1201$$
$$\times 7019 \times 823\ 543 \times 616\ 318\ 177 \times 6561 \times 100\ 895\ 598\ 169$$

est égal à 5 fois la somme de ses diviseurs propres, c'est-à-dire de tous les diviseurs de N sauf N. Si on note $\sigma(N)$ la somme de tous les diviseurs de N (y compris N lui-même), cela signifie que

$$\sigma(N) - N = 5N$$

ce qui est bien entendu équivalent à $\sigma(N) = 6N$. Nous allons calculer $\sigma(N)$ et voir comment, grâce à cela, Fermat a pu faire apparaître la factorisation de 100 895 598 169.

2.3 Calcul de σ (N)

Commençons par remarquer[3] que $169 = 13^2$, que $961 = 31^2$, que $6561 = 3^8$, que $823543 = 7^7$ et que $214748364800000 = 2^{36} \times 5^5$.

Nous pouvons en déduire que N se décompose de la façon suivante:

$$N = 2^{36} \times 3^8 \times 5^5 \times 7^7 \times 11 \times 13^2 \times 19 \times 31^2$$
$$\times 43 \times 61 \times 83 \times 223 \times 331 \times 379 \times 601$$
$$\times 757 \times 1201 \times 7019 \times 616318177 \times 100895598169$$

Hormis 100 895 598 169 dont on cherche la factorisation, tous les facteurs de cette décomposition de N sont des puissances de nombres premiers[4]. Tous ces facteurs sont donc premiers entre eux deux à deux et l'on peut supposer que les facteurs premiers de 100 895 598 169 sont distincts des autres facteurs premiers de N. Pour le voir rigoureusement, on peut faire successivement la division de 100 895 598 169 par 2, 3, 5, 7, ..., 7019 et 616 318 177 pour voir que le reste n'est jamais nul.

Savoir que ces facteurs sont premiers entre eux est important car on sait que la fonction σ est multiplicative, c'est-à-dire que $\sigma(mn) = \sigma(m)\sigma(n)$ dès lors que m et n sont premiers entre eux. Pour calculer $\sigma(N)$, il suffit donc de calculer les $\sigma(p^k)$ où p^k parcourt tous les facteurs de N donnés au-dessus. Mais cela est aisé car on sait que si p est premier, on a la formule $\sigma(p^k) = \dfrac{p^{k+1} - 1}{p - 1}$.

Voici donc le calcul de tous les $\sigma(p^k)$:

3. Ces décompositions se trouvent facilement car les facteurs premiers sont petits. Même si le dernier de ces nombres est grand, sa factorisation est facile, puisqu'après avoir divisé par 10^5, on s'aperçoit qu'on peut le diviser par deux jusqu'à trouver 1.

4. Le nombre 616 318 177, qui est premier, n'était pas inconnu de Fermat car c'est un diviseur du nombre de Mersenne $2^{37} - 1$. Fermat avait montré, dans une lettre à Mersenne datée de 1640 que $2^{37} - 1 = 223 \times 616318177$.

p^k	$\sigma(p^k)$
2^{36}	$2^{37}-1=223\times 616318177$
3^8	$9841=13\times 757$
5^5	$3906=2\times 3^2\times 7\times 31$
7^7	$960800=2^5\times 5^2\times 1201$
11	$12=2^2\times 3$
13^2	$183=3\times 61$
19	$20=2^2\times 5$
31^2	$993=3\times 331$
43	$44=2^2\times 11$
61	$62=2\times 31$
83	$84=2^2\times 3\times 7$
223	$224=2^5\times 7$
331	$332=2^2\times 83$
379	$380=2^2\times 5\times 19$
601	$602=2\times 7\times 43$
757	$758=2\times 379$
1201	$1202=2\times 601$
7019	$7020=2^2\times 3^3\times 5\times 13$
616318177	$616318178=2\times 7^3\times 898423$

Dans la dernière ligne apparaît le facteur 898 423, qui est premier. Fermat avait sans doute dû vérifier sa primalité.

Le nombre noté $\sigma(100895598169)$ ne peut pas être calculé pour le moment, donc on le notera s. On obtient la décomposition de $\sigma(N)$ en faisant le produit de tous les nombres de la colonne de droite et, après regroupement des termes, on obtient :

$$\begin{aligned}\sigma(N) = {} & 2^{30}\times 3^{9}\times 5^{5}\times 7^{7}\times 11\times 13^{2}\times 19\times 31^{2}\\ & \times 43\times 61\times 83\times 223\times 331\times 379\times 601\\ & \times 757\times 1201\times 898423\times 616318177\times s\end{aligned}$$

2.4 Un facteur commun à *N* et *σ(N)*

En regardant les décompositions de N et $\sigma(N)$, on se rend compte que le nombre

$$\begin{aligned}M = {} & 2^{30}\times 3^{8}\times 5^{5}\times 7^{7}\times 11\times 13^{2}\times 19\times 31^{2}\\ & \times 43\times 61\times 83\times 223\times 331\times 379\times 601\\ & \times 757\times 1201\times 616318177\end{aligned}$$

est un facteur commun à ces deux nombres. On peut donc écrire:

$$\begin{cases} N & = M\times 2^{6}\times 7019\times 100\ 895\ 598\ 169\\ \sigma(N) & = M\times 3\times 898\ 423\ \times s\end{cases}$$

Rappelons que la question posée à Fermat était d'étudier si $\sigma(N)$ est égal à un multiple de N. Si c'était le cas, on aurait $\sigma(N) = kN$ pour un certain entier k ce qui donnerait la relation:

$$M\times 3\times 898423\times s = k\times M\times 2^{6}\times 7019\times 100\ 895\ 598\ 169$$

Après simplification par M, cela implique que, soit le facteur premier 898 423 divise k, soit il divise 100 895 598 169. Cela a sans doute conduit Fermat à tenter de diviser 100 895 598 169 par 898 423, et il se trouve justement que cette division est exacte puisque 100 895 598 169 divisés par 898 423 égalent $112\ 303^{5}$ – ce qui donne à Fermat la deuxième partie de sa réponse à Mersenne.

5. Le nombre 112 303 est un premier.

2.5 Fin de la réponse…

A partir de là, Fermat pouvait répondre à la question globale de Mersenne qui était de savoir si la somme des diviseurs propres de N est un multiple de N. Si k est un entier tel que $\sigma(N) = kN$ alors

$$M \times 3 \times 898423 \times s = k \times M \times 2^6 \times 7019 \times 100895598169$$

ce qui donne, en simplifiant par M et par 898 423:

$$3 \times s = k \times 2^6 \times 7019 \times 112303$$

Or, $s = \sigma(100895598169) = \sigma(898423) \times \sigma(112303)$ donc

$$s = 898424 \times 112304 = (2^3 \times 112303) \times (2^4 \times 7019)$$

d'où:

$$3 \times 2^3 \times 112303 \times (2^4 \times 7019) = k \times 2^6 \times 7019 \times 112303$$

ce qui entraïne que $k = 6$. Ainsi, $\sigma(N) = 6N$ et donc, comme l'avait affirmé Fermat dans sa lettre en parlant de sous-quintuple des parties, on a bien $\sigma(N) - N = 5N$.

■

(juillet 2015)