Comment Fermat a-t-il factorisé 100 895 598 169 ?

blogdemaths.wordpress.com

Voici l'extrait d'une lettre de Fermat à Mersenne datant du 7 Avril 1643 :

> *« 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, 7 019, 823 543, 616 318 177, 6 561, 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.*
>
> *« Á 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.*
>
> *« Á la seconde question, je vous réponds que le dernier de ces nombres est composé et se fait du produit de ces deux : 898 493 et 112 303.*

Le but de ce document est d'expliquer la méthode qui a très probablement été utilisée par Fermat pour trouver la factorisation :

$$100\,895\,598\,169 = 898\,493 \times 112\,303$$

1 Quelques eclaircissements sur cette lettre

Dans l'extrait reporté ci-dessus, Fermat affirme que le nombre :

$$\begin{aligned} N =& 214748364800000 \times 11 \times 19 \times 43 \times 61 \times 83 \times 169 \\ & \times 223 \times 331 \times 379 \times 601 \times 757 \times 961 \times 1201 \\ & \times 7019 \times 823543 \times 616318177 \times 6561 \times 100895598169 \end{aligned}$$

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 $\sigma(N) = 6N$. Dans la suite, nous allons calculer $\sigma(N)$ et voir comment, grâce à cela, Fermat a pu faire apparaître la factorisation de 100 895 598 169.

2 Calcul de $\sigma(N)$

Commençons par remarquer [1] 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 :

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

1. Ces décompositions se trouvent facilement car les facteurs premiers sont petits.

Hormis 100 895 598 169 dont on cherche la factorisation, tous les facteurs de la décomposition de N sont des puissances de nombres premiers.[2] Tous ces facteurs sont donc premiers entre eux deux à deux (on peut supposer que les facteurs premiers de 100 895 598 169 sont disctincts des autres facteurs premiers de N. Pour le voir rigoureusement, on peut faire succesivement la division de 100 895 598 169 par 2, 3, 5, 7, ..., 7019 et 616 318 177 puis 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, $\sigma(p^k) = \frac{p^{k+1}-1}{p-1}$.

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	$616318178 = 2 \times 7^3 \times 898423$

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

2. Le nombre 616318177 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 $2^{37}-1 = 223 \times 616318177$.

Le nombre noté $\sigma(100\,895\,598\,169)$ 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 :

$$\begin{aligned}\sigma(N) =& 2^{30} \times 3^9 \times 5^5 \times 7^7 \times 11 \times 13^2 \times 19 \times 31^2 \\ & \times 43 \times 61 \times 83 \times 223 \times 331 \times 379 \times 601 \\ & \times 757 \times 1201 \times 898\,423 \times 616\,318\,177 \times s\end{aligned}$$

3 Un facteur commun à N et $\sigma(N)$

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

$$\begin{aligned}M =& 2^{30} \times 3^8 \times 5^5 \times 7^7 \times 11 \times 13^2 \times 19 \times 31^2 \\ & \times 43 \times 61 \times 83 \times 223 \times 331 \times 379 \times 601 \\ & \times 757 \times 1201 \times 616\,318\,177\end{aligned}$$

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 :

$$M \times 3 \times 898\,423 \times s = k \times M \times 2^6 \times 7019 \times 100\,895\,598\,169$$

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 112303. [3]

4 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

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

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

$$3 \times s = k \times 2^6 \times 7019 \times 112\,303$$

Or, $s = \sigma(100\,895\,598\,169) = \sigma(898\,423) \times \sigma(112\,303)$ donc

$$s = 898\,424 \times 112\,304 = (2^3 \times 112\,303) \times (2^4 \times 7019)$$

d'où :

$$3 \times 2^3 \times 112\,303 \times (2^4 \times 7019) = k \times 2^6 \times 7019 \times 112\,303$$

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

3. 112 303 est un nombre premier