Factorisations de grands nombres et machine de Carissan

Martine Bühler

On apprend dès l'école primaire à calculer le produit de deux nombres entiers, même grands, « à la main ». Mais l'opération inverse (factoriser un grand nombre entier) se révèle très ardue. Les mathématiciens se sont intéressés à ce problème, sans doute au départ comme à un défi intellectuel. On trouve ainsi dans les lettres de Fermat des indications à ce sujet.

La correspondance de Fermat

Les formes de l'activité mathématique au XVII^{ème} siècle ne sont pas unifiées. Il y a plusieurs sources de problèmes : traductions des œuvres de mathématiciens grecs (Euclide, Apollonius, Archimède, Diophante,…) ; navigation ; travaux des ingénieurs et artilleurs etc. Les publications mathématiques sont difficiles et assez rares, en particulier à cause de problèmes typographiques d'impression ; il n'y a pas de journaux scientifiques au début du dix-septième : ils feront leur apparition vers 1665, en même temps que l'Académie des Sciences. Fermat n'a jamais écrit de traité de théorie des nombres ; on connaît ses travaux à ce sujet par sa correspondance. A partir de 1636, par l'intermédiaire de Carcavi, son collègue au Parlement de Toulouse, Fermat rencontre le cercle de Mersenne et commence à correspondre avec ce dernier. Mersenne est un personnage essentiel de l'époque[1] ; il échange des lettres sur de multiples sujets philosophiques et scientifiques avec des correspondants de l'Europe entière : Roberval, Pascal, Hobbes, Descartes, Gassendi,… Il a plusieurs centaines de correspondants en Europe et même jusqu'en Turquie. Les lettres sont recopiées, réexpédiées, remaniées. Les mathématiciens s'envoient des problèmes, des solutions, des défis. Les lettres de Fermat que nous allons examiner sont des réponses à un défi de Mersenne.

Lettre de Fermat à Mersenne du mardi 7 avril 1643
Extrait des *Œuvres*, ed. Tannery et Henry, tome II, 1894

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,
1 201, 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.

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.

Je suis toujours, mon Révérend Père,

Votre très humble et très affectionné serviteur,
FERMAT.

A Toulouse, ce 7 avril 1643.

Cette lettre mérite quelques explications. Une partie aliquote d'un entier N est un diviseur de N différent de N. On cherche la proportion d'un nombre N avec ses parties aliquotes, c'est-à-dire avec la somme s(N) de ses diviseurs différents de lui-même (le diviseur 1 étant compris). La réponse de Fermat stipule que s(N) = 5N. Nous donnons dans l'annexe 1 des indications permettant d'obtenir ce résultat. Fermat affirme ensuite que 100 895598169 = 898 423 x 112 303, résultat stupéfiant[2]. Il ne donne cependant pas ici de méthode générale de factorisation mais seulement la réponse. Dans une autre lettre, qu'on imagine postérieure mais sans pouvoir précisément la dater, Fermat propose une méthode. Nous allons étudier cette lettre de près.

Lettre de Fermat à Mersenne (1643)
Extrait des *Œuvres*, ed. Tannery et Henry, tome II, 1894

[1] Le Père Marin Mersenne (1588-1648) a fait ses études chez les Jésuites au collège de la Flèche puis est entré chez les Minimes.

[2] Vous pouvez vérifier : c'est juste ! La TI89 donne cette factorisation quand on utilise le programme Factor mais la TI92 reste persuadée que N est premier, tout en calculant correctement le produit des deux facteurs.

Tout nombre impair non quarré est différent d'un quarré par un quarré, ou est la différence de deux quarrés, autant de fois qu'il est composé de deux nombres, et, si les quarrés sont premiers entre eux, les nombres compositeurs le sont aussi. Mais si les quarrés ont entre eux un commun diviseur, le nombre en question sera aussi divisible par le même commun diviseur, et les nombres compositeurs seront divisibles par le côté de ce commun diviseur.

Par exemple : 45 est composé de 5 et de 9, de 3 et de 15, de 1 et de 45. Partant, il sera trois fois la différence de deux quarrés : savoir de 4 et de 49, qui sont premiers entre eux, comme aussi sont les compositeurs correspondants 5 et 9 ; plus, de 36 et de 81, qui ont 9 pour commun diviseur, et les compositeurs correspondants, 3 et 15, ont le côté de 9, savoir 3, pour commun diviseur ; enfin 45 est la différence de 484 et 529, qui ont 1 et 45 pour compositeurs correspondants.

Il est fort aisé de trouver les quarrés satisfaisants, quand on a le nombre et ses parties, et d'avoir les parties lorsqu'on a les quarrés.

Pour nous, il s'agit de l'application d'une identité remarquable et on peut faire lire ce texte à des élèves de troisième. Si $N = a^2 - b^2$ avec a et b entiers, alors $N = (a + b) \times (a - b)$ et $N = p.q$ avec $p = a + b$ et $q = a - b$ entiers. Réciproquement si un nombre entier impair N est égal à un produit d'entiers p.q, alors p et q sont tous deux impairs et $N = \left(\frac{p+q}{2}\right)^2 - \left(\frac{p-q}{2}\right)^2$ avec $\left(\frac{p+q}{2}\right)$ et $\left(\frac{p-q}{2}\right)$ entiers. Il est donc équivalent de factoriser un nombre entier impair ou de le mettre sous forme de différence de deux carrés. Ayant à factoriser un grand nombre, par exemple N = 2 027 651 281, on cherche a et b tels que $N = a^2 - b^2$. On cherche donc un nombre entier a tel que $a^2 - N$ est un carré parfait ; on commence les recherches à $a = E(\sqrt{N}) + 1$ car c'est la première valeur de a qui rend $a^2 - N$ positif. Ensuite on essaie a + 1, a + 2, a + 3,…jusqu'à ce que cela marche. La suite du texte, que vous trouverez dans la rubrique *Dans nos classes* page 53,avec un problème bâti à partir du texte, donne un algorithme de calcul[3] qui permet d'éviter les élévations au carré dans la recherche de a et b. Fermat factorise ainsi 2 027 651 281 en douze étapes alors que la méthode « naturelle » par divisions successives aurait nécessité d'essayer tous les nombres premiers jusqu'à 44 021. Dans ce cas, la méthode proposée par Fermat est donc nettement plus efficace que la méthode courante. Quand cela se produit-il exactement ?

Lorsque $N = a^2 - b^2$, le nombre d'étapes de l'algorithme de Fermat est $a - (Ent(\sqrt{N}) + 1)$ c'est-à-dire si on revient aux facteurs p et q de N environ $\frac{p+q}{2} - \sqrt{pq} = \frac{\left(\sqrt{p} - \sqrt{q}\right)^2}{2}$. La méthode est donc particulièrement efficace si les facteurs p et q de N sont « proches ». On peut se demander si Fermat a utilisé sa méthode pour factoriser 100 895 598 169 dans sa réponse au défi de Mersenne ; le nombre d'étapes nécessaires est alors 187 721 et il y a fort à parier qu'il a procédé autrement. Tannery, dans son édition des œuvres de Fermat, donne une indication sur la procédure peut-être employée, développée dans l'annexe 1.

Qu'en est-il si N est premier ? Alors la seule décomposition possible est N = N.1 donc $a = \frac{N+1}{2}$. La méthode permet donc d'affirmer que N est premier si la seule solution trouvée est $a = \frac{N+1}{2}$ mais le nombre d'étapes est alors à peu près $\frac{N+1}{2} - \sqrt{N} = \frac{\left(\sqrt{N} - 1\right)^2}{2}$ et en tant que test de primalité la méthode n'est pas efficace.

Fermat ramène donc le problème de la factorisation d'un grand nombre à celui de savoir si un nombre entier est ou non un carré. Il fait alors une remarque qui aura de l'avenir : il est immédiat que certains nombres **ne sont pas des carrés** car les carrés, en numération décimale, ne se termine pas par n'importe quoi ; par exemple, 49 619 ne peut pas être un carré *parce que aucun carré* ne finit par 19. Ainsi, l'inspection des « finales » permet d'éliminer un grand nombre de valeurs de a car on voit immédiatement que $a^2 - N$ n'est pas un carré. C'est cette remarque que vont généraliser les frères Carissan pour mécaniser l'algorithme de résolution.

La machine des frères Carissan

Pierre et Eugène Carissan sont nés respectivement en 1871 et 1880. Pierre Carissan devient professeur de mathématiques en 1896 et Eugène Carissan sort de Saint-Cyr. Pierre collabore à la revue de mathématiques amusantes *Le Sphinx-Œdipe* et s'intéresse à la construction d'une machine à congruences réalisée par son frère Eugène ; la machine étant peu performante, les deux frères imaginent des améliorations. Le travail s'interrompt pendant la Première Guerre Mondiale. Eugène reprend la fabrication après la guerre et la machine est finalement

[3] L'étude détaillée de cet algorithme est faite dans le devoir donné en terminale S comme aide à la lecture du texte.

construite en 1919. Un article est publié dans le *Bulletin de la Société d'Encouragement à l'Industrie Nationale* en 1920 pour expliquer le principe et le fonctionnement de la machine.

Le problème des frères Carissan est la résolution d'équations en nombres entiers. L'idée est d'éliminer des valeurs impossibles de par leur résidu modulo m pour certaines valeurs du module m. Il s'agit bien d'une généralisation de la remarque de Fermat sur les « finales » car cela revenait à éliminer certaines valeurs à cause de leur résidu modulo 100. La machine des frères Carissan est donc utile pour résoudre un grand nombre d'équations diophantiennes[4] et en particulier, elle peut nous aider à trouver x et y tels que $N = x^2 - y^2$. Travaillons par exemple[5] modulo 7 et cherchons les résidus quadratiques modulo 7, c'est-à-dire les carrés modulo 7 :

x	0	1	2	3	4	5	6
x^2	0	1	4	2	2	4	1

Les résidus quadratiques modulo 7 sont 0, 1, 2, 4 et les non-résidus sont 3, 5, 6. Ceci signifie que, si un nombre est congru à 3, 5 ou 6 modulo 7, **il ne peut pas être un carré**. S'il est congru à 0, 1, 2 ou 4, tout est possible : il peut être un carré ou ne pas en être un. Reprenons notre problème de factorisation et cherchons à factoriser 250 507. Il s'agit donc de trouver x tel que $x^2 - 250\,507$ est un carré. On a : $N \equiv 5$ (mod 7) donc $x^2 - 5$ doit être un carré modulo 7 donc $x^2 - 5$ doit être congru à 0 ou 1 ou 2 ou 4 modulo 7. Donc x^2 doit être congru à 5 ou 6 ou 0 ou 2 modulo 7 ; comme x^2 est un carré, les seules valeurs possibles pour x^2 sont 0 ou 2 donc x doit être congru à 0 ou 3 ou 4 modulo 7. Les valeurs 0, 3, 4 sont appelées *valeurs possibles* modulo 7.

L'idée de la machine de Carissan est d'éliminer un grand nombre de valeurs de x en travaillant sur 14 modules simultanément. Examinons le principe de la machine de Carissan avec un modèle fonctionnant avec trois modules : 7, 9 et 15. Faisons avec 9 et 15 un travail semblable à celui effectué avec le module 7.

Carrés modulo 9 :

x	0	1	2	3	4	5	6	7	8
x^2	0	1	4	0	7	7	0	4	1

Carrés modulo 15 :

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
x^2	0	1	4	9	1	10	6	4	4	6	10	1	9	4	1

On a : $N \equiv 1 \pmod 9$ donc $x^2 - 1$ doit être un carré modulo 9 donc $x^2 - 1$ est congru à 0 ou 1 ou 4 ou 7 modulo 9 donc x^2 est congru à 1 ou 2 ou 5 ou 8 modulo 9 ce qui donne comme valeurs permises pour x modulo 9 : 1 ou 8.

Et enfin $N \equiv 7 \pmod{15}$ donc $x^2 - 7$ doit être congru à 0 ou 1 ou 4 ou 6 ou 9 ou 10. Donc x^2 est congru à 7 ou 8 ou 11 ou 13 ou 1 ou 2 donc les valeurs permises pour x modulo 15 sont : 1 ou 4 ou 11 ou 14.

Vous trouverez dans l'annexe 2 quatre pages, qui, photocopiées sur transparent, vous permettront de réaliser une machine de Carissan rétroprojetable[6] formée de trois disques matérialisant les restes de x dans les divisions par 7, 9 et 15. Plaçons sur chaque disque des gommettes sur les valeurs possibles pour x ; puis nous mettons la machine en position initiale correspondant à x = 501 car $501 = E(\sqrt{N}) + 1$. Nous alignons donc les valeurs 4, 6, 6 sur la ligne marquée **position initiale**. Tournons chaque disque d'un cran : les valeurs alignées sur la **position initiale** sont maintenant les valeurs de 502 modulo 7, 9 et 15. On continue à tourner et, lorsqu'on obtient trois gommettes alignées sur la **position initiale**, le nombre correspondant pour x a de bonnes chances de convenir car il est une valeur possible pour les modules 7, 9 et 15. Mais attention ! Ce n'est pas sûr et il faut vérifier à la main que cela marche bien.

Voici les valeurs successives obtenues :

mod7	4	5	6	0	1	2	3	4	5	6	0	1	2	**3**
mod9	6	7	8	0	1	2	3	4	5	6	7	8	0	**1**
mod15	6	7	8	9	10	11	12	13	14	0	1	2	3	**4**

[4] C'est-à-dire d'équations dont les inconnues sont des nombres entiers.

[5] Rappelons que deux entiers a et b sont congrus modulo 7 (noté $a \equiv b \pmod 7$) si et seulement si 7 divise a – b ; tout entier est congru à son reste dans la division par 7 et on peut donc travailler avec les restes possibles, c'est-à-dire 0, 1, 2, 3, 4, 5 et 6. Enfin, les opérations « passent » aux congruences et si $x \equiv y \pmod 7$ alors $x^2 \equiv y^2 \pmod 7$.

[6] Pour réaliser la machine rétroprojetable, attacher les trois disques grâce à une attache parisienne fixée en leur centre, puis fixer cette attache sur la ligne « position initiale » du quatrième transparent.

Nous stoppons la machine après 14 essais (le premier compris) car nous obtenons trois valeurs permises. Essayons alors :

$$x = 501 + 13 = 514.$$
$$x^2 - N = 514^2 - 250\,057 = 13\,689 = 117^2.$$
$$\text{Donc } 250\,507 = (514 + 117)(514 - 117) = 631 \times 397.$$

La machine de Carissan permet de travailler sur 14 modules : 19, 21, 23, 26, 29, 31, 34, 37, 41, 43, 47, 53, 55 et 59. Elle comporte 14 couronnes comportant le nombre de plots correspondant à chacun de ces 14 modules. Pour résoudre notre problème de factorisation, il faut donc chercher les valeurs possibles de x dans chacun de ces modules. Ensuite, on place un capuchon sur les plots des valeurs possibles et on met la machine en position initiale pour le premier essai (501 dans notre exemple). Une manivelle permet de faire tourner les couronnes et lorsqu'on obtient 14 capuchons alignés, on tient une solution possible (mais pas sûre) : il faut alors faire un calcul « à la main » pour vérifier qu'on a bien une solution.

Avec sa machine, Carissan a montré que $2^{21} - 1$ est premier et a factorisé 3 570 537 526 921 en 841 249 x 4 244 329 ; il n'a pas utilisé la méthode de Fermat mais des résultats sur la représentation de nombres entiers avec des formes quadratiques et en particulier la représentation des nombres sous forme de somme de deux carrés. Nous ne développerons pas ici ces théories, qui feront peut-être l'objet d'un autre conte du lundi.

La méthode du crible quadratique

Dans l'article de *Pour la Science* cité en bibliographie, Johannes Buchmann explique une méthode moderne de factorisation utilisant les mêmes idées. Si on cherche à factoriser un nombre N, on cherche deux nombres x et y tels que $x^2 - y^2 \equiv 0 \pmod N$ avec $x \neq \pm y \pmod N$. (Remarquons que cela n'est possible que si N n'est pas premier car, si N est premier, « N divise $x^2 - y^2$ » entraîne « N divise x –y ou N divise x + y »). Si N divise $x^2 - y^2$ sans diviser x – y ni x + y alors un diviseur propre p de N divise x – y et un autre diviseur propre q de N divise x + y . Donc P.G.C.D.(x – y, N) ≠ 1 et il suffit de calculer P.G.C.D.(x – y, N) par l'algorithme d'Euclide pour trouver un diviseur de N différent de 1 et de N. Le problème est donc de trouver x et y convenables.

La méthode du crible quadratique consiste à choisir une base de nombres premiers $\{p_1, p_2, p_3, ..., p_n\}$ avec laquelle on va travailler. Dans une première étape, on cherche des nombres a tels que a^2 est « proche » de N (dans un sens qu'on précisera plus tard) tels que a^2-N admette uniquement les nombres de la base choisie comme facteurs premiers. Nous allons appliquer la méthode à N = 125 249. La base choisie est $\{2, 3, 5, 7, 11, 13\}$. E(√N) = 353 donc on prendra a « proche » de 353. Le tableau suivant montre le « crible » appliqué : pour chaque valeur de a, on a mis dans la ligne de chaque facteur premier choisi la puissance à laquelle il intervient dans la décomposition de $a^2 - N$; la case reste vide s'il n'intervient pas ; enfin, dans la dernière ligne, figure le facteur restant quand on a divisé $a^2 - N$ par tous les nombres premiers de la base ; si ce nombre est 1, alors a nous convient car $a^2 - N$ admet comme seuls diviseurs premiers ceux de la base choisie, sinon la valeur est à rejeter.

a	347	348	349	350	351	352	353	354	355	356	357
$a^2 - N$	-4840	-4145	-3448	-2749	-2048	-1345	-640	67	776	1487	2200
-1	-1	-1	-1	-1	-1	-1	-1				
2	2^3		2^3		2^{11}		2^7		2^3		2^3
3											
5	5	5					5				5^2
7											
11	11^2										11
13											
	1	829	431	2749	**1**	269	**1**	354	97	1487	**1**

Il y a donc dans ce cas 4 valeurs convenables. On écrit alors les décompositions obtenues :

$$L_1 : 347^2 - N = (-1) \times 2^3 \times 5 \times 11^2$$
$$L_2 : 351^2 - N = (-1) \times 2^{11}$$
$$L_3 : 353^2 - N = (-1) \times 2^7 \times 5$$
$$L_4 : 357^2 - N = 2^3 \times 5^2 \times 11$$

Il faut ensuite choisir certaines lignes qu'on va multiplier entre elles ; le but est d'obtenir dans le membre de droite uniquement des exposants pairs. Pour cela on résout un système d'équations linéaires dans **Z/2Z** : on affecte en effet à chaque ligne un coefficient λ_i égal à 1 si on prend la ligne et à 0 si on ne la prend pas ; l'exposant de 2 obtenu dans le membre de droite par la multiplication des lignes est alors

$3\lambda_1 + 11\lambda_2 + 7\lambda_3 + 3\lambda_4$; il faut donc trouver un quadruplet $\{\lambda_1, \lambda_2, \lambda_3, \lambda_4\}$ tel que les exposants obtenus pour –1 et pour 2, 5, 11(seuls nombres premiers intervenant ici) soient tous pairs, c'est-à-dire nuls dans **Z/2Z** . De plus, $3\lambda_1 + 11\lambda_2 + 7\lambda_3 + 3\lambda_4$ est pair si et seulement si $3\lambda_1 + 11\lambda_2 + 7\lambda_3 + 3\lambda_4 \equiv 0 (\text{mod } 2)$ c'est-à-dire si $\lambda_1 + \lambda_2 + \lambda_3 + \lambda_4 = 0$ dans **Z/2Z**. On obtient ainsi un système de 4 équations à 4 inconnues dans **Z/2Z**.

$$\begin{cases} \lambda_1 + \lambda_2 + \lambda_3 = 0 \\ \lambda_1 + \lambda_2 + \lambda_3 + \lambda_4 = 0 \\ \lambda_1 + \lambda_3 = 0 \\ \lambda_4 = 0 \end{cases}$$

On a réduit tous les coefficients modulo 2. La résolution du système donne : $\begin{cases} \lambda_2 = 0 \\ \lambda_4 = 0 \\ \lambda_1 + \lambda_3 = 0 \end{cases}$ et on choisit comme solution $\begin{cases} \lambda_1 = \lambda_3 = 1 \\ \lambda_2 = \lambda_4 = 0 \end{cases}$. La multiplication des lignes L_1 et L_3 donne alors :

$(347^2 - N)x(353^2 - N) = (-1)^2 \times 2^{10} \times 5^2 \times 11^2$

Donc : $347^2 \times 353^2 \equiv (2^5 \times 5 \times 11)^2 \ (\text{mod}N)$

Or $347 \times 353 \equiv 122491 \equiv -2758 \ (\text{mod}N)$ et $2^5 \times 5 \times 11 = 1760$. On obtient alors : $2758^2 \equiv 1760^2 \ (\text{mod}N)$. Donc N divise $2758^2 - 1760^2 = (2758 + 1760)x(2758 - 1760)$ sans diviser l'un des facteurs. Un diviseur propre de N divise alors 2758 – 1760 = 998. On applique l'algorithme d'Euclide pour trouver P.G.C.D.(N,998).

$$125\,249 = 125 \times 998 + 499$$
$$998 = 2 \times 499$$

On a : P.G.C.D.(N,998) = 499. On tient un diviseur de N.

$$125\,249 = 499 \times 251.$$

Pour factoriser un nombre de 50 chiffres, il faut une base de facteurs premiers comportant 3000 nombres premiers ; il en faut 51 000 pour un nombre de 100 chiffres.

Le problème de la factorisation des grands nombres et du temps de calcul pour y parvenir est revenu sur le devant de la scène avec la cryptographie moderne : la sécurité du système R.S.A. repose sur la difficulté (présumée) de factoriser rapidement de très grands nombres[7].

[7] voir conte du lundi p 31 dans ce numéro.

Annexe 1 : somme des diviseurs d'un nombre

On note : $\sigma(N)=\sum_{d/N} d$ la somme des diviseurs d'un nombre entier N (y compris N).

Si le nombre p est premier, on a $\sigma(p)=1+p$ et $\sigma(p^\alpha)=1+p+p^2+...p^\alpha$.

Si p et q sont deux nombres premiers distincts, on a alors :

$$\begin{aligned}\sigma(p^\alpha)\times\sigma(q^\beta) &= (1+p+...+p^\alpha)\times(1+q+...+q^\beta)\\ &= 1+p+...+p^\alpha+q+pq+...p^\alpha q+...q^\beta+q^\beta p+...q^\beta p^\alpha\\ &= \sum_{\substack{0\le i\le\alpha\\ 0\le j\le\beta}} p^i q^j=\sigma(p^\alpha q^\beta)\end{aligned}$$

On obtient ainsi, lorsque
$N=p_1^{\alpha_1}\times p_2^{\alpha_2}\times...\times p_n^{\alpha_n}$ où les p_i sont premiers avec $p_i\neq p_j$, $\sigma(N)=\sigma(p_1^{\alpha_1})\times\sigma(p_2^{\alpha_2})\times...\times\sigma(p_n^{\alpha_n})$

Et de même, si m et n sont premiers entre eux : σ(m.n) = σ(m)σ(n).

On peut alors s'attaquer au problème posé par Mersenne à Fermat et à la réponse[8] de celui-ci dans sa lettre du 7 avril 1643. On cherche la somme des diviseurs de
N = 241 748 364 800 000 x 11 x 19 x 43 x 61 x 83 x 169 x 223 x 331 x 379 x 601 x 757 x 1201 x 7019 x 823 543 x 616 318 177 x 6561 x 100 895 598 169
241 748 364 800 000 = 2^{36} x 5^5 et il n'y a pas d'autre facteur 2 ou 5 dans N. En fait, les facteurs de N donnés par Mersenne sont premiers deux à deux donc on cherche la somme des diviseurs de chacun d'eux pour obtenir la somme des diviseurs de N.
$\sigma(2^{36})=1+2+...2^{36}=2^{37}-1=137438953471=223\times616318177$ Or 616 318 177 est un facteur premier qu'on retrouve dans N, ce qui va faciliter le calcul de $\frac{\sigma(N)}{N}$.

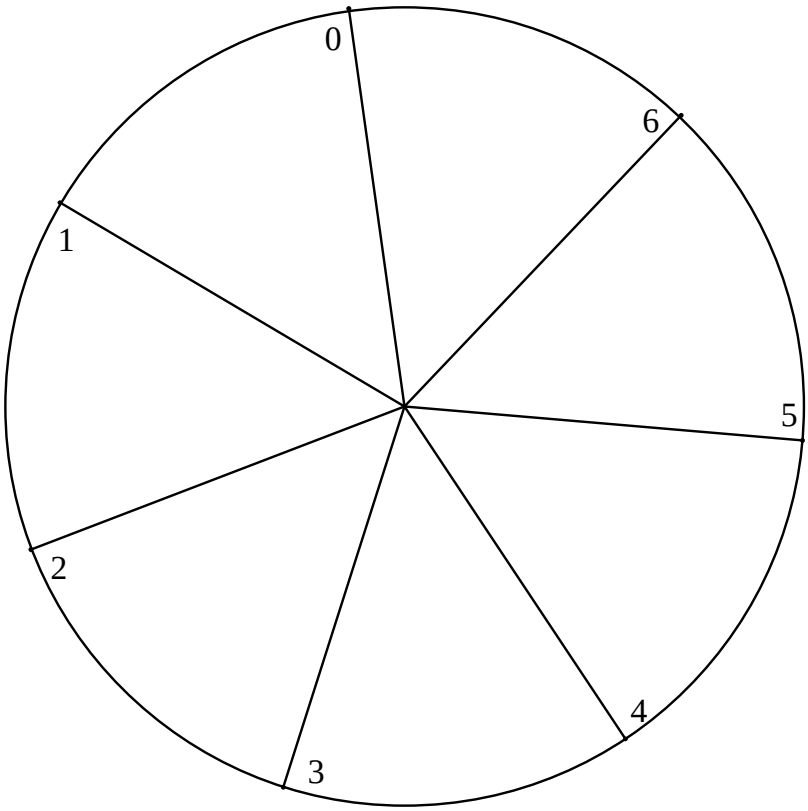
σ(11) = 12 =2^2x3
σ(19) = 20 = 2^2x 5
σ(43) = 2^2 x 11
σ(61) = 62 = 2 x 31
σ(83) = 84 = 2^2 x 3 x 7
σ(169) = σ(13^2) = 1 + 13+ 13^2 = 3 x 61
σ(223) = 224 = 2^5 x 7
σ(331) = 332 = 2^2 x 83
σ(379) = 380 = 2^2 x 5 x 19
σ(601) = 602 = 2 x 7 x 43
σ(757) = 758 = 2 x 379
σ(961) = σ(31^2) = 1 + 31 + 31^2 = 993 = 3 x 331
σ(1201) = 1202 = 2 x 601
σ(7019) = 7020 = 2^2 x 3^3 x 5 x 13
σ(6561) = σ(3^8) = (3^9 – 1)/2 = 13 x 757
σ(823 543) = σ(7^7) = (7^8 – 1)/6 = 2^5 x 5^2 x 1201
σ(616 318 177) = 616 318 178 = 2 x 7^3 x 898 423
Reste à trouver σ(100 895 598 169)et donc la décomposition de 100 895 598 169. Or tous les facteurs trouvés dans les sommes de diviseurs déjà calculés sont des facteurs de N sauf 898 423. Fermat a dû raisonner comme un bon élève qui, devant un problème qu'on lui demande de résoudre, pense qu'il doit être résoluble ! Or, ici, si on veut pouvoir calculer σ(N)/N, il serait bien pratique que 898 423 divise N. Essayons donc de voir s'il divise le dernier facteur de N. Or, justement, en essayant, on trouve la décomposition de ce fameux 100 895 598 169 , c'est-à-dire : 898 423 x 112 303. Par la même occasion, terminons le calcul de la somme des diviseurs :
σ(898 423) = 898 424 = 2^4 x 112 303 et σ(112 303) = 112 304 = 2^4 x 7019

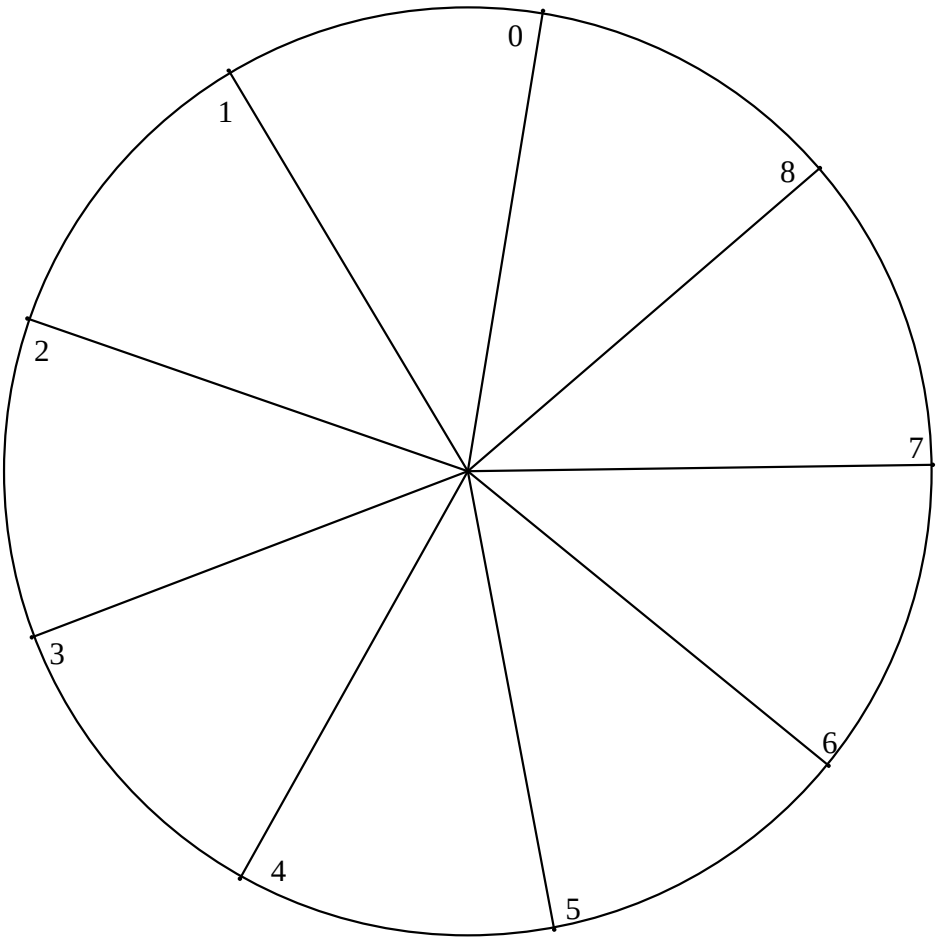
[8] La méthode suivie est celle suggérée par Tannery dans l'édition des œuvres de Fermat citée en bibliographie.

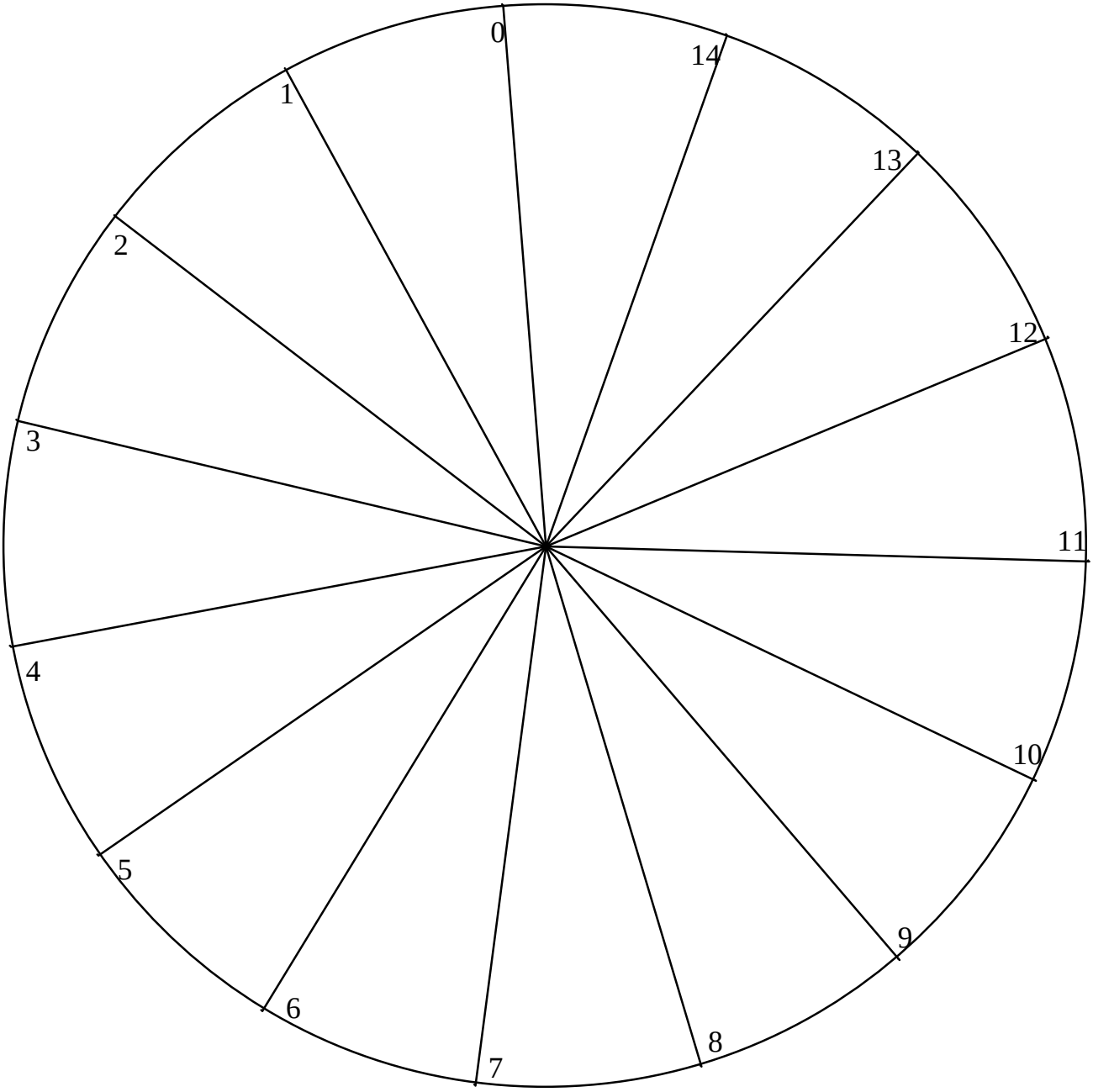
On peut dire que cela tombe merveilleusement bien puisqu'on retrouve des facteurs de N. On peut maintenant trouver $\sigma(N)/N = 2 \times 3 = 6$.

Fermat, lui, s'occupe de la somme des parties aliquotes, c'est-à-dire de $s(N) = \sum_{\substack{d / N \\ d \neq N}} d = \sigma(N) - N$. Donc s(N) = 5N ; N est sous-quintuple de ses parties aliquotes et, en cours de calcul, on a trouvé la factorisation de 100 895 598 169.

Annexe 2 : machine de Carissan rétroprojetable à trois disques


0
6
1
5
2
4
3


0
1
8
2
7
3
6
4
5


0
14
1
13
2
12
3
11
4
10
5
9
6
8
7

Bibliographie

P. FERMAT *Œuvres*, éd. Tannery et Henry, 1894, pp. 257-258

E. CARISSAN *Machine à résoudre les congruences*, Bulletin de la Société d'Encouragement à l'Industrie Nationale, n°132, 1920.

F. MORAIN *La machine de Carissan*, Pour la Science, janvier 1998.

F. MORAIN, J.O. SHALLIT, H.C. WILLIAMS *La machine à congruences*, La Revue n°14, Musée des Arts et Métiers Editions, mars 1996.

J. BUCHMANN *La factorisation des grands nombres*, Pour la Science, n°251, septembre 1998.

J.P. DELAHAYE *La cryptographie R.S.A. vingt ans après*, Pour la Science, n°267, janvier 2000.

Un film d'une quinzaine de minutes a été réalisé sur la machine de Carissan avec le Musée des Arts et Métiers ; ce film peut être emprunté à la bibliothèque de l'I.R.E.M. Paris VII.