Factorisation de grands nombres : de Fermat à la machine des frères Carissan

Martine Bühler(*)

On apprend dès l'école primaire à calculer le produit de deux nombres, même grands. Mais comment décomposer un nombre, par exemple 16 837, en un produit (autre que $1 \times 16\,837$) ? Les mathématiciens se sont intéressés à ce problème, au départ comme à un défi intellectuel.

Au début du siècle, deux frères, Pierre et Eugène Carissan, cherchent à mécaniser les calculs pour ce problème. Pierre, professeur de mathématiques, s'intéresse à la construction d'une machine à congruences qui sera réalisée par son frère Eugène. Le travail s'interrompt pendant la première Guerre Mondiale et la machine est finalement construite en 1920.

L'origine de la méthode qui mènera à la construction de la machine de Carissan remonte au XVII^{e} siècle. Dans une lettre écrite en 1643 au Père Marin Mersenne, Pierre de Fermat explique une méthode générale permettant de factoriser de grands nombres. Il remarque qu'il revient au même de mettre un nombre sous forme de produit ou de différence de deux carrés. Il donne l'exemple de 45 :

$$45 = 81 - 36 = 9^2 - 6^2 = (9 + 6) \times (9 - 6)$$
$$45 = 15 \times 3$$

Ceci n'est que l'application d'une « identité remarquable » :

$$N = x^2 - y^2 = (x + y)\,(x - y)$$

Il montre ensuite comment la méthode s'applique à de grands nombres. Essayons avec 16 837. On cherche deux nombres x et y tels que $16\,837 = x^2 - y^2$ c'est-à-dire tels que $y^2 = x^2 - 16\,837$. Il s'agit donc de trouver un nombre x tel que $x^2 - 16\,837$ est un carré. Il faut donc que x^2 soit supérieur à 16 837 ; on commencera les recherches avec $x = 130$. Ensuite, il est parfois immédiat que certains nombres ne sont pas des carrés car un carré se termine obligatoirement par 0, 1, 4, 5, 6 ou 9 ; il ne se termine jamais par 2, 3, 7 ou 8 ; aucun calcul n'est donc nécessaire pour savoir par exemple que 213 n'est pas un carré. Ceci permet de limiter les calculs.

$130^2 - 16\,837 = 63$ n'est pas un carré. $x = 130$ ne convient pas. Continuons !

$131^2 - 16\,837 = 324 = 18^2$. On a gagné !

$16\,837 = 131^2 - 18^2 = (131 + 18) \times (131 - 18) = 149 \times 113$.

En deux essais seulement, nous avons factorisé 16 837. Si nous avions cherché par la méthode « naturelle » de divisions successives, il aurait fallu examiner si 16 837 était divisible par 2, 3, 5, 7, 11, etc. jusqu'à 113. C'eût été beaucoup plus long !

Dans sa lettre à Mersenne, Fermat factorise en douze étapes 2 027 651 281.

Le problème de factoriser un nombre se ramène ainsi à celui de savoir reconnaître

(*) Groupe M. :A.T.H. IREM Paris VII

si un nombre est un carré. Les frères Carissan vont mécaniser cette recherche de nombres carrés à l'aide des congruences. Travaillons par exemple(1) 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 N = 250 507. II s'agit donc de trouver x tel que $x^2 - 250\,507$ soit un carré. On a $N \equiv 5 \pmod 7$ 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. Nous allons expliquer ce que serait une machine de Carissan 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 l ou 4 ou 6 ou 9 ou l0. 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.

Durant l'atelier que j'ai animé à Lille en 2001, nous avons fait fonctionner une machine rétroprojetable formée de trois disques matérialisant les restes de x dans les divisions par 7, 9 et 15, pour factoriser N = 250 507. Nous avons placé sur chaque disque des gommettes sur les valeurs possibles pour x, puis mis la machine en position initiale correspondant à $x = 501$ car $501 = \mathrm{ENT}(\sqrt{N}) + 1$. Nous alignons

(1) 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 $x^2 \equiv y^2 \pmod 7$.

donc les valeurs 4, 6, 6 sur une 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:

mod 7	4	5	6	0	1	2	3	4	5	6	0	1	2	3
mod 9	6	7	8	0	1	2	3	4	5	6	7	8	0	1
mod 15	6	7	8	9	10	11	12	13	14	0	1	2	3	4

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

$$X = 501 + 13 = 514.$$

$$X^2 - N = 514^2 - 250\,057 = 13\,689 = 117^2.$$

Donc

$$250\,057 = (514 + 117)(514 - 117) = 631 \times 397.$$

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. Durant l'atelier de Lille, nous avons visionné un film d'une quinzaine de minutes (qu'on peut emprunter à l'IREM Paris VII) montrant le fonctionnement de la machine sur l'exemple 250 507.

Un article plus complet sur la question paraîtra dans le numéro 17 de la revue *Mnémosyne*, publiée par le groupe M. :A.T.H. à l'IREM Paris VII.

Bibliographie

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

E. CARISSAN. *Machine à résoudre les congruences*, Bulletin de la Société d'Encouragement à l'industrie Nationale, nº 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 nº 14, Musée des Arts et Métiers Éditions, mars 1996.

J. BUCHMANN. *La factorisation des grands nombres*, Pour la Science, nº 251, septembre 1998.

J.-P. DELAHAYE. *La cryptographie R.S.A. vingt ans après*, Pour la Science, nº 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.