



La machine des frères Carissan

FRANÇOIS MORAIN

À la recherche des machines qui décomposaient les grands nombres en facteurs premiers.

Pourquoi est-il facile de multiplier deux nombres entiers et si ardu de trouver deux entiers dont le produit est donné ? Le problème de la factorisation occupe les mathématiciens depuis longtemps ; dès le XIX^e siècle, ils ont cherché à construire des machines facilitant les calculs répétitifs et fastidieux de la factorisation.

Dans certaines branches de la théorie des nombres, les calculs peuvent être assez aisément automatisés. C'est le cas des cribles. Le plus connu d'entre eux est le crible d'Ératosthène, qui permet de trouver tous les nombres premiers dans un intervalle donné (on écrit tous les nombres de 0 à 100, par exemple ; on élimine ensuite tous les multiples de 2, puis tous les multiples de 3, puis de 5, etc ; après avoir passé tous les nombres «au crible», on ne conserve ainsi que 2, 3, 5, 7, 11, 13, etc. qui sont premiers). Une extension de cette notion de crible permet de résoudre les équations en nombres entiers du type $N = x^2 - y^2$: c'est le cas de la méthode de Fermat (voir l'encadré). La méthode est efficace quand

les diviseurs ont des valeurs voisines et elle est adaptable à des dispositifs mécaniques.

Le mathématicien anglais Frederick Lawrence semble avoir été le premier à préconiser la construction d'un crible pour factoriser des entiers, en 1896. Bien qu'il ait écrit comment fabriquer une telle machine, elle ne vit pas le jour. L'idée de Lawrence fut oubliée jusqu'en 1910, quand André Gérardin publia une traduction française de son article dans sa revue de «mathématiques amusantes», *Sphinx-Ceïpe*. Cet article semble avoir inspiré à l'ingénieur Maurice Kraitchik, l'idée de construire un prototype d'une telle machine, en 1912.

Pierre Carissan, professeur de mathématiques est aussi rédacteur à la revue *Sphinx-Ceïpe*, et il s'intéresse à la fabrication d'une telle machine. Après avoir occupé différents postes de professeur de mathématiques, il est nommé, en 1914, au Collège Dumont-d'Urville, près de Caen. Certains de ses proches le considèrent comme un «original fini».

Son frère, Eugène Olivier, entre à l'École spéciale militaire, en 1900. En

1912, les deux frères construisent une machine à factoriser les grands nombres, mais ni leur prototype, ni celui de Kraitchik ne donne de résultats intéressants. Eugène entreprend la fabrication d'un nouveau prototype en 1913, mais le projet est interrompu par la guerre.

Héroïque, il est blessé trois fois durant la guerre (en juillet 1915, il refuse même d'être évacué et continue à se battre). Après la guerre, il est nommé professeur à l'École militaire de Saint-Maixent, et reprend la construction de la machine, dite machine à congruences. Elle sera achevée en 1919 par la maison *Château Frères*, spécialisée dans la fabrication d'instruments scientifiques. Elle permettra la résolution de plusieurs problèmes de la théorie des nombres.

Eugène Carissan meurt en 1925 sans avoir eu le temps de faire exécuter les modifications qu'il jugeait nécessaires. Il voulait notamment entraîner la machine par un petit moteur électrique et non plus à la main. Aucune modification n'est entreprise, et la machine disparaît.

À LA RECHERCHE DE LA MACHINE DE CARISSAN

Avec mes collègues Jeffrey Shallit, à l'Université canadienne de Waterloo et Hugh Williams, à l'Université du Manitoba, nous apprenons l'existence de la machine des frères Carissan à l'automne 1989. Sherlock Holmes des mathématiques, nous cherchons la machine dans toute la France : nous enquêtons pour retrouver la maison *Château Frères*, et visitons les musées techniques français. La première piste aboutit rapidement à une impasse : la maison *Château Frères* n'existe plus. Les pistes du Conservatoire national des arts et métiers, de l'École normale supérieure, de l'Institut Henri Poincaré ou encore de la Bibliothèque nationale échouent.

Après une année de recherches infructueuses, J. Shallit décide d'employer les grands moyens : avec l'aide de Jean-Paul Allouche, de l'unité CNRS URA 410, il écrit à tous les Carissan de

La factorisation de 611

Supposons que l'on veuille factoriser 611. S'il existe deux nombres x et y tels que $611 = x^2 - y^2$, on peut alors factoriser la différence :

$$611 = x^2 - y^2 = (x - y)(x + y)$$

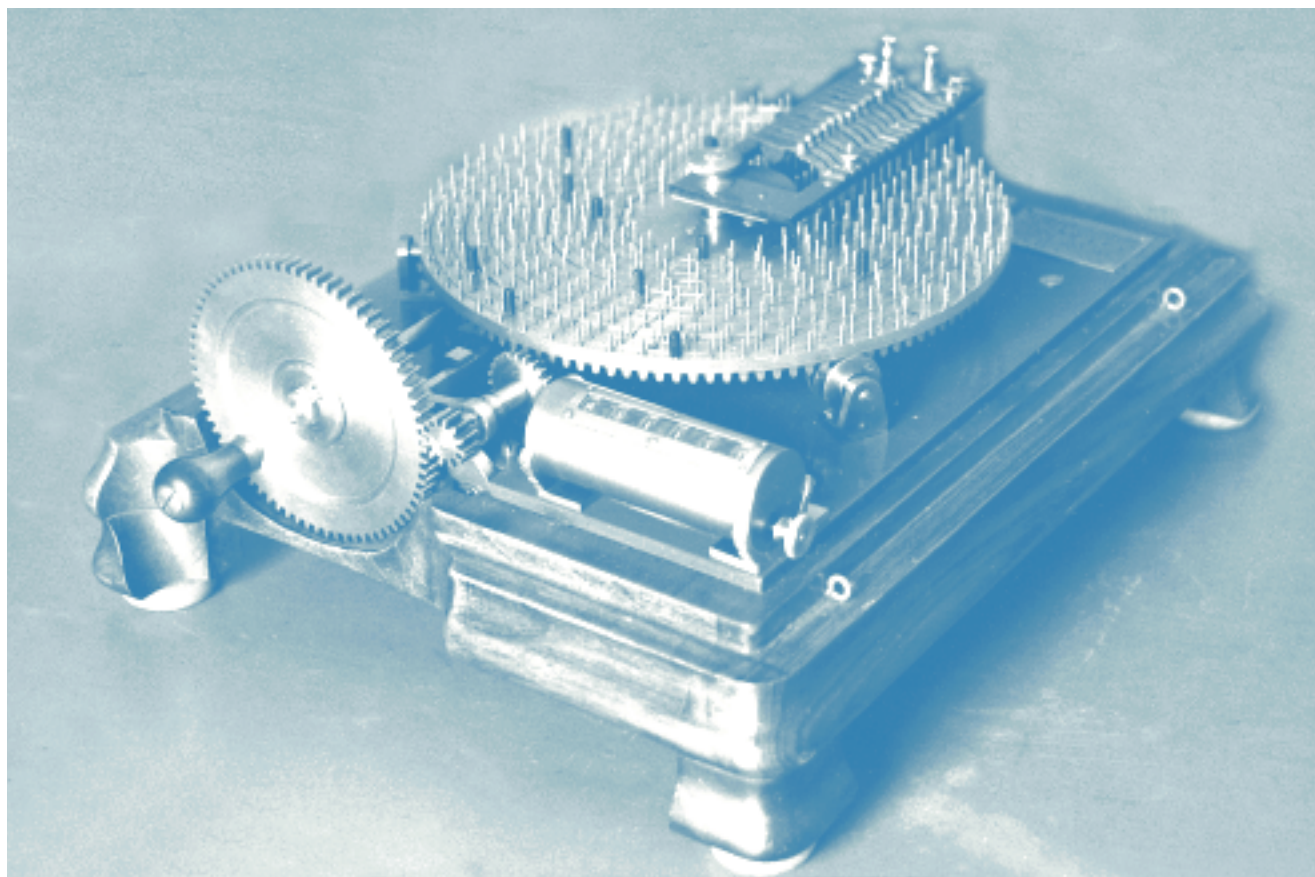
Pour trouver x et y , on fait varier x et on cherche à quelles conditions $x^2 - 611$ est un carré parfait. Pour que cette expression soit un carré, il faut que $x^2 - 611$ soit positif, de sorte que l'on commence la recherche à partir du nombre immédiatement supérieur à la racine carrée de 611, soit 25.

On essaye alors les nombres 26, 27, 28, etc. jusqu'à trouver une valeur de x pour laquelle $x^2 - 611$ est le carré d'un entier. Pour $x = 30$, on obtient :

$$x^2 - 611 = 289 = 17^2 ; \text{ on en déduit que } 611 = 30^2 - 17^2 = (30 - 17)(30 + 17) = 13 \times 47.$$

On limite le nombre d'essais en rassemblant les conditions que doit remplir $x^2 - 611$ pour être un carré parfait. Ainsi, le carré d'un entier, en base 10, doit nécessairement se terminer par 0, 1, 4, 5, 6, ou 9.

Quand on essaye $x = 27$, on obtient $x^2 - 611 = 118$ qui, terminé par un 8, n'est pas un carré parfait : 27 n'est pas acceptable. Les frères Carissan ont généralisé la méthode : leur machine, permettait de trouver les carrés parfaits, égaux à $x^2 - N$, où N est le nombre à factoriser (voir la figure de la page suivante).



Hugh Williams

La machine à congruences des frères Carissan. Une manivelle fait tourner la roue dentée qui entraîne d'une part un compteur et d'autre part 14 couronnes de laiton, chacune avançant d'un picot à l'autre pour la rotation d'une dent de pignon (le compteur avance d'une unité à chaque rotation d'une dent). Avant de tourner la roue, toutes les couronnes sont en position «0». À chaque couronne est associé un nombre (19, 21, 23, 26, 29, 31, 34, 37, 41, 43, 47, 53, 55 et 59) matérialisé par autant de picots. Soit N le nombre à factoriser. On utilise la relation $N = x^2 - y^2$ et l'on cherche les conditions que doit remplir x pour

que y^2 soit un carré parfait. Si des valeurs permises de x sont 1, 7, 8, 13, 14 et 20 modulo 21, on place un capuchon métallique sur les picots n° 1, 7, 8, etc. de la couronne 21. De même pour les autres couronnes utilisées. On tourne la manivelle et quand les capuchons métalliques (les plots noirs) des différentes couronnes sont alignés, un contact électrique s'établit sous la barrette métallique, et un signal retentit. Le nombre indiqué sur le cadran a alors des chances d'être un carré parfait. La machine factorise des nombres de treize chiffres en moins de 18 minutes, tâche qui demanderait plusieurs jours à la main.

France et de Navarre pour leur demander s'ils connaissent la machine que nous recherchons. Au cours de l'été 1991, les 85 Carissan référencés sur notre liste reçoivent une lettre, où on leur demande tous les renseignements possibles sur cette machine et sur ses inventeurs.

Les premières réponses ne tardent pas à arriver, mais elles sont toutes décevantes. Enfin, nous recevons un appel téléphonique d'une des filles d'Eugène Carissan : la machine existe toujours et elle est entreposée près de Bordeaux. Apparemment, la machine est restée en possession de la famille jusque vers 1940, quand Jean Dubois, astronome et ami de la famille Carissan, la fit transférer à l'Observatoire de Floirac, près de Bordeaux. Elle y a été entreposée jusqu'en 1992.

Elle fonctionne parfaitement bien. La famille de l'inventeur, étonnée de voir trois chercheurs remuer ciel et terre pour retrouver la machine due au génie paternel a donné la machine au Conservatoire national des arts et métiers, où elle est désormais installée.

Avons-nous achevé – avec les honneurs – notre carrière de détectives ? Non, car il existe d'autres machines, notamment celle d'Édouard Lucas. On doit à ce mathématicien français les premières méthodes permettant de montrer de façon rigoureuse la primalité des entiers. Son résultat le plus connu est le test qu'il a établi pour prouver la primalité des nombres de Mersenne, c'est-à-dire des nombres que l'on peut écrire sous la forme $M_n = 2^n - 1$. Aujourd'hui, les programmes utilisés de par le monde pour trouver le plus grand nombre premier utilisent tous le test de Lucas (les mathématiciens trouvent régulièrement un nouveau « plus grand nombre premier » : le plus récent est $M_{2976221} = 2^{2976221} - 1$, composé de 895 932 chiffres).

Lucas aurait utilisé son théorème pour prouver, à la main, la primalité de M_{127} , un nombre de 39 chiffres en base 10. Cela aurait représenté quelque 300 heures de travail. En fait, pour tester la primalité des nombres de Mersenne, Lucas s'est servi d'un échiquier inspiré des métiers à tis-

ser qui le fascinaient : il faisait glisser les lignes de chiffres à la façon dont le peigne tasse la laine sur le métier. Il y travaillait en base 2 : les 1 étaient représentés par des pions et les 0 par des cases vides.

En 1887, il écrivit qu'Henri Genaille, ingénieur aux Chemins de fer français et lui construisaient une machine mécanique pour tester la primalité des nombres de Mersenne (un « piano arithmétique »). Ils ont aussi collaboré à l'invention de plusieurs dispositifs de calcul, dont beaucoup sont au Musée du Conservatoire national des arts et métiers.

Malheureusement, Lucas est mort accidentellement, quelques semaines après cet article, à l'issue d'un banquet, et l'on a perdu la trace de la machine construite par Genaille et Lucas. Peut-être dort-elle dans quelque grenier ?

François MORAIN, ingénieur de l'armement, enseigne l'informatique à l'École Polytechnique.