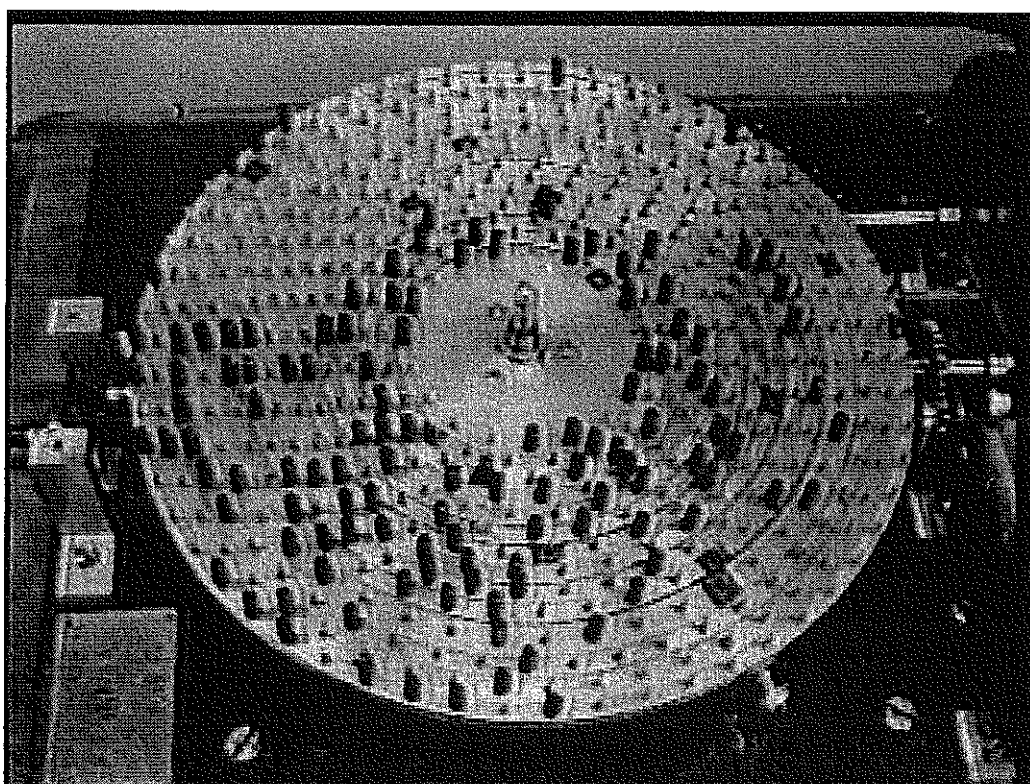


BONNES VIEILLES PAGES

Nous présentons ici le texte intégral de l'article d' Eugène Carissan paru en 1920 dans le *Bulletin de la Société d'Encouragement à l'Industrie Nationale*, article dans lequel il explique le fonctionnement de sa machine à congruences¹. Ci-dessous, une photographie de la machine de Carissan, prise au Musée des Arts et Métiers.



¹ Pour plus de précisions, voir l'étude page 15 de ce numéro.

MACHINE A RÉSOUDRE LES CONGRUENCES⁽¹⁾

But. — Cet appareil, qui a figuré à l'Exposition de machines à calculer organisée par la Société d'Encouragement du 5 au 13 juin 1920, a pour but la résolution mécanique, en nombres entiers, des équations indéterminées à deux variables.

Principe. — La machine est une application de la théorie des congruences, et des méthodes d'utilisation de cette théorie qu'a instituées M. André Gérardin, de Nancy (2), pour la résolution des équations indéterminées.

Soit, à titre d'exemple simple, à résoudre en nombres entiers l'équation :

$$x^2 - 6y^2 = 1\,324\,801 = A$$

ou

$$6y^2 + A = x^2. \quad (1)$$

On envisage successivement les diverses hypothèses possibles : $y = \text{mult. de } m + 0, 1, 2, \dots (m-1)$, pour un certain nombre de diviseurs ou modules m , et on examine dans chacune de ces hypothèses s'il y a compatibilité entre le premier et le deuxième membre de l'équation (1), en tenant compte de ce fait que x^2 ne peut avoir, pour un module déterminé, que certaines valeurs connues à l'avance (résidus quadratiques).

Soit à appliquer le module 5; on a, en remarquant que A est un mult. de $5 + 1$, et que les résidus quadratiques (valeurs de x^2) ne peuvent être, en module 5, que 0, 1, 4 :

1^{re} hypothèse :

$y = \text{mult. de } 5 + 0$; $6y^2 = \text{mult. de } 5 + 0$; $6y^2 + A = \text{mult. } 5 + 1 \dots$ combinaison possible.

2^e et 3^e hypothèses :

$y = \text{mult. de } 5 \pm 1$; $6y^2 = \text{mult. de } 5 + 1$; $6y^2 + A = \text{mult. } 5 + 2 \dots$ — impossible.

3^e et 4^e hypothèses :

$y = \text{mult. de } 5 \pm 2$; $6y^2 = \text{mult. de } 5 + 4$; $6y^2 + A = \text{mult. } 5 + 0 \dots$ — possible.

En résumé, y ne peut être que mult. de $5 + 0$; mult. de $5 + 2$; mult. de $5 + 3$, ce que nous exprimons par la *bande modulaire* 01001, dans laquelle : le signe 0 marque la possibilité, le signe 1 l'impossibilité.

(1) Communication faite en séance publique par l'auteur le 26 juin 1920.

(2) Directeur de la revue : *Le Sphinx-OEdipe*, 32, Quai Claude-Le-Lorrain, Nancy.

De même, appliquons le module 7 (en remarquant que A est un mult. de $7 + 2$, et que x^2 , en module 7, ne peut être égal qu'à 0, 1, 2, 4) :

1^{re} hypothèse :
 $y = \text{mult. de } 7 + 0$; $6y^2 = \text{mult. de } 7 + 0$; $6y^2 + A = \text{mult. de } 7 + 2 \dots$ combinaison possible.
 2^e et 7^e hypothèses :
 $y = \text{mult. de } 7 \pm 1$; $6y^2 = \text{mult. de } 7 + 6$; $6y^2 + A = \text{mult. de } 7 + 1 \dots$ — possible.
 3^e et 6^e hypothèses :
 $y = \text{mult. de } 7 \pm 2$; $6y^2 = \text{mult. de } 7 + 3$; $6y^2 + A = \text{mult. de } 7 + 5 \dots$ — impossible.
 4^e et 5^e hypothèses :
 $y = \text{mult. de } 7 \pm 3$; $6y^2 = \text{mult. de } 7 + 5$; $6y^2 + A = \text{mult. de } 7 + 0 \dots$ — possible.

Bande modulaire correspondante : 0010010.

En opérant pareillement avec d'autres modules, 11, 13, 17..., on obtiendrait d'autres bandes modulaires, comportant également d'autres conditions pour y . Or, un nombre quelconque est un multiple du module $m + 0, 1, 2, 3, \dots (m - 1)$, c'est-à-dire correspond à l'une des cases de la bande modulaire en m . Il sera *solution* si les cases auxquelles il correspond sur les bandes des différents modules comportent, toutes à la fois, le signe de possibilité.

Le rôle d'une *machine* propre à rechercher cette solution sera donc de juxtaposer toutes les bandes modulaires établies, en faisant correspondre les cases de même rang, et d'avertir l'opérateur lorsqu'à un rang déterminé, toutes les bandes comporteront le signe de possibilité. Pour ce faire, la machine doit renouveler automatiquement la bande de chaque module, dès qu'elle a été utilisée.

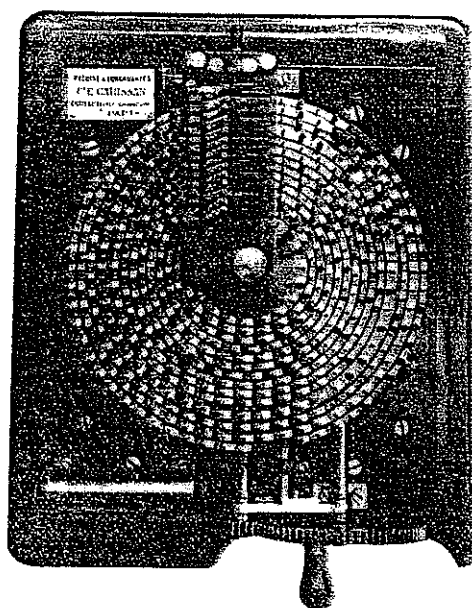
Le tableau suivant montre la disposition des bandes juxtaposées, au moment où apparaît la première solution de l'équation (1) autre que 0.

Série naturelle des nombres .	135	136	137	138	139	140	141	142	143	144
Module 5	0	I	0	0	I	0	I	0	0	I
— 7	I	0	0	I	0	0	0	I	0	0
— 11	0	I	0	0	I	0	I	0	0	0
— 13	0	I	I	0	I	0	I	0	0	0
— 17	I	0	I	0	I	0	I	I	0	0
— 19	I	0	I	0	I	0	0	I	I	0
c'est-à-dire $y = 140$, correspondant à $x = 1201$.										

Historique. — Indépendamment des machines personnelles de M. Gérardin, et de celle envisagée par M. Kraitchik, un premier modèle de machine basée sur le principe théorique ci-dessus fut conçu en 1912 par M. P. Carissan, professeur au collège de Lesneven; ce modèle, construit par le lieutenant

E. Carissan, et présenté au Congrès de Nîmes de l'Association française pour l'Avancement des Sciences, en 1912, par M. Gérardin, utilisait des bandes modulaires fermées, souples, pendantes, entraînées simultanément par un même cylindre cannelé, avec décodage optique des solutions : mais le rendement était faible.

En 1913-1914, le lieutenant Carissan conçoit et construit de ses mains un



1. — L'appareil monté vu en plan.

premier modèle de la machine à congruences actuelle : les résultats sont si encourageants, qu'ils paraissent justifier les frais d'une construction de précision, laquelle fut confiée à la Maison Château Frères, de Paris. La guerre interrompit cette construction, et l'appareil définitif du commandant E. Carissan ne put être achevé qu'à la fin de 1919.

Description de la machine du commandant E. Carissan (fig. I et II). — Des couronnes métalliques concentriques, figurant les bandes modulaires, sont soutenues dans le même plan horizontal par trois lignes de galets à 120°. Elles sont dentées sur leur face inférieure : les dentures, toutes de même pas, sont taillées de manière

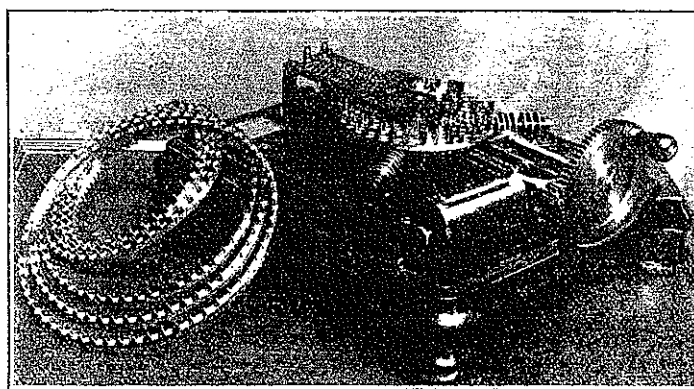
que les couronnes puissent être toutes entraînées simultanément (mais non avec la même vitesse) par un même long pignon dont l'axe est parallèle au plan des couronnes, et passe par leur axe de rotation commun.

Chaque couronne porte, vissées normalement sur sa face supérieure, des broches d'acier *équidistantes*. Les nombres de ces broches, portées par les différentes couronnes, sont les nombres premiers jusqu'à 39 (modules). Les dents inférieures de chaque couronne sont en nombre *double*. De la sorte, il est possible, en choisissant les dents des couronnes mises en prise avec le pignon entraîneur, de réaliser *l'alignement des broches suivant un rayon*, prolongement de celui suivant lequel les couronnes sont en prise.

Lorsque le pignon entraîneur tourne sur son axe, les couronnes tournent concentriquement toutes à la fois *du même nombre de dents*, et l'alignement radial des broches se renouvelle, au moment où elles passent sur le rayon fixe, dit *ligne d'investigation*.

Chaque couronne figurant une bande modulaire, les *possibilités* sont représentées par de petites *coiffes* de fibre, enfilées sur les broches voulues. Les alignements des broches se succédant par la rotation des couronnes sont donc composées de broches garnies et non garnies de coiffes. Lorsque un alignement ne comporte que des coiffes, il y a *solution*.

Décel automatique des solutions. — La machine avertit lorsqu'un tel alignement passe sur la ligne d'investigation. L'organe préposé à ce décel ou *herse* est composé d'une série de petits marteaux de cuivre, de forme demi-cylindrique, portés par des ressorts légers, montés sur une plaquette de fibre,



II. — Vue perspective de l'appareil (des couronnes modulaires ont été retirées pour montrer le dispositif d'entraînement).

au-dessus des passages respectifs des broches des différentes couronnes. A chaque marteau correspond une coupure d'un circuit électrique sur lequel sont montés en série une pile sèche et un récepteur téléphonique.

Lorsqu'une coiffe passe sous la herse, comme sa hauteur est un peu plus grande que celle de la broche qui lui sert de support, le marteau correspondant est soulevé, et sa coupure annulée. Quand tous les marteaux sont soulevés à la fois, toutes les coupures, qui sont en série, sont annulées à la fois, et le courant passe. L'opérateur est averti par un *toc* caractéristique du téléphone.

Détails du mécanisme. — Couronnes. — Afin de réduire à la fois le frottement mutuel des couronnes et leurs déplacements latéraux, chacune d'elles est pourvue, sur sa face inférieure, et à côté de la denture, d'un chemin de roulement pour les galets qui lui servent de support.

Les broches de chaque couronne sont numérotées 1, 2, 3, ... m . L'origine (m) de chaque couronne est peinte en rouge; sa moitié marquée d'un repère noir.

Afin d'obtenir un encombrement minimum, et plus d'uniformité dans la largeur des couronnes modulaires (largeur qui est commandée par le nombre des côtés du polygone régulier, *de côté constant*, à y inscrire), les différentes couronnes représentent — du centre à la périphérie — les modules :

19, 3×7 , 23, 2×13 , 29, 31, 2×17 , 37, 41, 43, 47, 53, 5×11 , 59, c'est-à-dire 17 modules répartis sur 14 couronnes, les bandes correspondant aux modules composés (2×13 , 2×17 , 3×7 , 5×11) étant obtenues par la combinaison des modules simples.

Embrayage et débrayage. — Une manette extérieure permet d'embrayer ou de déembrayer simultanément toutes les couronnes, par effacement du pignon entraîneur. Ce dispositif permet : de rendre folles les couronnes, ce qui rend plus aisé le placement préalable des coiffes; le cas échéant, de placer, avant de mettre la machine en marche, chaque couronne dans la position qu'elle occuperait si l'appareil avait déjà fonctionné jusqu'à une valeur donnée. En un mot, ce dispositif permet de commencer l'investigation à partir d'un nombre arbitraire, si grand soit-il, en s'épargnant une révolution dont l'inutilité aurait été reconnue *a priori*.

Compteur. — Un compteur, allant jusqu'à 10^6 , et commandé par le pignon d'entraînement, donne à chaque instant le rang de la ligne de broches passant sur la ligne d'investigation. Il est à apparition brusque des chiffres, et comporte un organe de débrayage et de remise au zéro.

Commande de la machine. — Elle se fait à la main, par l'intermédiaire d'un volant denté multiplicateur. Un dispositif de commande par moteur électrique, avec rupture automatique du circuit du moteur, et arrêt (par l'intermédiaire d'un relai) du fait même du passage d'une solution, est à l'étude.

Récepteur téléphonique. — Pour plus de commodité, le récepteur téléphonique est remplacé par un *casque* téléphonique; dans ces conditions, la netteté du signal acoustique est telle que l'opérateur n'a nul besoin de concentrer son attention pour être à coup sûr averti, quelle que soit la rapidité de rotation de la machine.

Disposition d'ensemble. — L'ensemble de la machine est porté par un socle en ébénisterie, reposant sur cales de caoutchouc. Un couvercle en tôle laquée, qui s'emboîte sur la platine de l'appareil, protège ses organes contre la poussière.

Utilisation de la machine. — Les bandes modulaires étant établies pour l'équation à résoudre, débrayer la machine, placer les coiffes sur les broches

voulues de chaque couronne, en s'aidant du numérotage. Deux cas peuvent alors se présenter :

1° *L'investigation doit commencer à partir de zéro* : placer les repères rouges sous la herse, ce qui amène les repères noirs à former une ligne continue (au-dessus de la ligne d'entraînement par le pignon);

2° *L'investigation doit commencer à partir d'un nombre N* : dans ce cas, déterminer d'abord les restes (résidus) de la division de N par les modules qu'utilise la machine (19, 21, 23... 59), et placer chaque couronne de manière que le nombre, résidu correspondant à son module, soit sur la ligne d'investigation.

Dans les deux cas, les couronnes une fois placées, embrayer. Mettre le compteur au zéro, puis mettre en place le dispositif avertisseur téléphonique, en serrant sous les bornes *ad hoc* les extrémités du circuit pile-casque téléphonique. L'opérateur, muni du casque, n'a plus alors qu'à tourner à vitesse modérée (2 tours à la seconde) le volant d'entraînement. Lorsqu'une solution « passera », ce dont le téléphone avertira, arrêter la rotation sans brutalité, revenir en arrière doucement, en observant les alignements, jusqu'au moment où le toc se reproduit. Lire alors le compteur qui donne la valeur cherchée (ajouter le nombre N s'il y a lieu).

Puissance et rendement de la machine. — Les nombres de broches portées par les différentes couronnes étant premiers entre eux, la machine ne reproduira exactement une même disposition initiale relative des couronnes que quand elle aura examiné un nombre d'unités égal au produit des modules entre eux, qui est un nombre de 22 chiffres. Pratiquement, la *puissance* de la machine peut donc être considérée comme illimitée.

Il est prévu que des nombres satisfaisant à l'ensemble des conditions imposées par les bandes modulaires, et qui sont par conséquent livrés par la machine, peuvent ne pas être solutions de l'équation proposée. (Ces nombres, ou *pseudo-solutions*, auraient été éliminés par la mise en jeu de modules supplémentaires.) Mais étant donné le nombre des couronnes, la probabilité pour qu'un nombre fourni par la machine soit solution réelle est considérable.

Le temps nécessaire pour l'obtention d'une solution est extrêmement variable suivant les équations, depuis quelques secondes jusqu'à plusieurs heures. Des équations n'admettant *aucune* solution entière peuvent être soumises à la machine : celle-ci restera alors indéfiniment muette.

Le *rendement* de la machine est normalement de 35 à 40 nombres examinés à la seconde, soit de 2 000 à 2 400 à la minute. La rapidité de rotation ne compromet pas la netteté du signal avertisseur, bien que la durée du courant qui produit ce dernier ne soit pas supérieure à $\frac{1}{250}$ de seconde.

Applications de la machine. — La machine permet l'obtention directe des solutions entières des équations à deux variables, de la forme générale :

$$f(x) = \varphi(y).$$

La grandeur et le signe des coefficients et des exposants — pourvu qu'ils soient entiers — sont indifférents.

Son emploi est indiqué pour toutes les équations de cette sorte pour lesquelles l'existence et la valeur des solutions ne pouvant être prévues par la théorie des nombres, la résolution doit être recherchée par la voie expérimentale.

En particulier, l'appareil est appliqué avec succès à la décomposition des grands nombres, la recherche des nombres premiers, et l'étude de leur répartition.

L'intérêt de la machine reste, jusqu'à nouvel ordre, purement spéculatif. Mais il n'est nullement démontré que l'astronomie, par exemple, ne puisse retirer de son emploi un bénéfice positif.

Exemples de questions traitées avec la machine.

Résoudre :

$$\begin{aligned} x^2 - 13y^2 &= 1 \text{ (pour } x < 10\,000) \\ x &= 649; \quad y = 180. & (5 \text{ minutes}) \\ 2u^2 + v^2 &= 708\,158\,977 \\ u &= 14\,676; \quad v = 16\,655. & (8 \text{ minutes}) \\ x^2 - 6y^2 &= 1\,451^2 \text{ (pour } x \text{ et } y < 13\,000) \\ x &= 0, 1\,201, 7\,685; \quad y = 0, 140, 3\,102. & (7 \text{ minute}) \\ x^3 \pm y^3 &= 736\,249\,048 \\ x &= 919, -271; \quad y = \pm 271, \pm 919. & (8 \text{ minutes}) \end{aligned}$$

* *

Mettre sous la forme de la somme de deux carrés :

$$\begin{aligned} 708\,158\,977 &= 19\,224^2 + 18\,401^2. & (10 \text{ minutes}) \\ 1\,321\,442\,641 &= 25\,704^2 + 23\,703^2. & (15 \text{ minutes}) \\ 18\,403\,321\,661 &= 95\,930^2 + 95\,931^2. & (1 \text{ heure}) \end{aligned}$$

* *

Reconnaître si les nombres suivants sont premiers : le cas échéant, donner leurs facteurs ;

$A = 62\,080\,247$. Réponse affirmative : ne peut être mis que d'une seule façon sous la forme $x^2 - 2y^2$ ($x = 9\,005$, $y = 3\,083$, qui sont premiers entre eux) (3 minutes de rotation).

$A = 225\,058\,681$. Réponse négative : $A = 1\,909^2 + 14\,880^2$ et $A = 5\,741^2 + 13\,860^2$, d'où l'on tire : $A = 229 \times 982\,789$ (5 minutes).

$A = 3\,450\,315\,321$. Réponse négative : $A = 2\,975^2 + 58\,664^2$ et $A = 3\,664^2 + 58\,625^2$, d'où l'on tire : $A = 2\,448\,769 \times 1\,409$ (2 minutes).

$A = 2^{31} - 1 = 2\,147\,483\,647$. Réponse affirmative, en employant successivement deux méthodes (17 minutes et 15 minutes) :

$A = 65\,535^2 - 2 \times 32\,767^2$. Seule décomp. de cette forme, facteurs premiers entre eux.

$A = 4 \times 23\,081^2 + 3 \times 2\,349^2$. Seule décomp. de cette forme, facteurs premiers entre eux.

$A = 3\,570\,537\,526\,921$. Réponse négative. Le point de départ de l'investigation a été $1\,336\,000$, voisin de la racine carrée de A . La machine a donné en 18 minutes les deux décompositions :

$A = 1\,336\,139^2 + 1\,336\,140^2$ et $A = 1\,370\,700^2 + 1\,300\,661^2$, d'où l'on tire : $3\,570\,537\,526\,921 = 841\,249 \times 4\,244\,329$.

COMMANDANT E. CARISSAN.