29

Histoire et application des machines de crible numérique

Hugh C. Williams
University of Manitoba, Winnipeg

[résumé par Abalo Baya]

Une machine est dite *machine crible* si elle permet de résoudre un ou plusieurs systèmes de congruences linéaires à une variable. Le mécanisme de résolution de tels systèmes est la recherche exhaustive sur un ensemble d'entiers fixé. Une telle approche peut paraître naïve, mais pour certains problèmes, on ne connaît pas de méthode plus efficace. Dans cet exposé l'auteur fait l'historique sur les machines cribles et montre comment elles ont été utilisées pour obtenir des informations portant sur divers problèmes relatifs à la théorie des nombres.

Intéressons-nous d'abord à l'un des problèmes fondamentaux de l'exposé. On se donne

1. un intervalle $[A, B]$ avec $B > A$,
2. k entiers $m_1, m_2, \ldots, m_k$ premiers entre eux ($m_i > 1, i = 1, 2, \ldots, k$) appelés les "modulos",
3. k ensembles de résidus

$$R_i = \{r_{ij} \mid 0 \leq r_{ij} < m_i\},\ i = 1,\ 2,\ \ldots, k.$$

Le problème consiste à trouver tous les x tels que $A \leq x < B$ et $x \bmod m_i \in R_i$, $i = 1, 2, \ldots, k$. Certains cas particuliers classiques de ce problème peuvent être résolus à l'aide d'un algorithme efficace (c'est par exemple le cas du problème des restes chinois qui se résout à l'aide de l'algorithme d'Euclide), alors que pour les autres on ne connaît pas de méthode plus efficace que la résolution par des machines cribles. Les premières machines cribles de résolution d'une équation diophantienne par la méthode d'exclusion (Gérardin, Kraitchic, P. & E. Carissan (1912)) sont restées à l'état de prototype. La machine crible de Carissan (1919) est à commande manuelle et utilise 14 modulos dans la méthode d'exclusion : elle trie 35 à 40 nombres par seconde. Quant au crible optique de Lehmer (1932), il atteint une performance de 5000 tris par seconde. Par ailleurs, Lehmer a construit une machine automatique pouvant résoudre certains problèmes de crible et cette méthode a permis de factoriser des grands entiers tels que $(2^{136} + 1)/98564897$. Jusqu'à 1970, cette méthode était la plus efficace connue pour la factorisation des entiers. Le tableau suivant donne pour chaque machine, l'année de sa réalisation, le nombre de modulos utilisés et sa performance en nombres de tris par seconde.

Machine	année	nb. modulos	nb. tris/s
E. Carissan	1919	14	35 – 40
"Bicycle Chain"	1926	19	50
"Optical Gears"	1932	30	5000
"16 mm Movie Film"	1936	18	50
A. Gérardin	1937	?	?
SWAC	195x	?	1450
IBM7094	196x	21 ou 22	100000
DLS-127	1966	31	1000 000
DLS-157	1969(?)	37	1000 000
ILLIAC IV	196x	64	15 000 000
Registre à Décalage	1975	42	20 000 000
UMSU	1983	32	133 000 000
SSU	1991	30	200 000 000

Comme application, ces machines ont été utilisées pour le calcul des polynômes quadratiques dont les valeurs comportent une forte densité de nombres premiers, pour la recherche de la solution du problème des pseudo-carrés et du problème d'Erdős. Dans la dernière partie de l'exposé, l'auteur présente un dispositif de crible qu'il a mis au point pour la recherche du plus grand pseudo-carré. La performance d'un tel dispositif est de 8.87×10^{11} tris par seconde.

Références

[1] E. Carissan. *London Math. Soc. Lecture Notes*, 154:38–75.