Théorème des restes chinois et interpolation polynomiale

Isaac J. Schoenberg
Août 1986

Université du Wisconsin-Madison
Centre de recherches en mathématiques

Pour des entiers donnés a_i $(1 \leq i \leq n)$ et des entiers positifs m_i $(1 \leq i \leq n)$ premiers entre eux deux à deux, le problème des restes chinois Problem (abrégé en P.R.C.) peut s'énoncer comme suit :

Problème. *Trouver un entier x satisfaisant les congruences*

$$x \equiv a_i \pmod{m_i}, \quad (i = 1, 2, ..., n) \tag{1}$$

Si on a trouvé une solution x alors clairement, toutes les solutions de (1) appartiennent à une classe de congruence modulo $M = m_1 m_2 \dots m_n$.

Un jour dans les années 50, le défunt mathématicien hongro-suédois Marcel Riesz était en visite à l'Université de Pennsylvanie et il nous dit de manière informelle qu'on peut penser au P.R.C. (1) comme à un analogue de l'interpolation par des polynômes : étant données des valeurs réelles y_i $(1 \leq i \leq n)$ et des valeurs réelles distinctes x_i, trouver un polynôme $P(x)$ de degré $\leq n-1$ tel que

$$P(x_i) = y_i, \quad (i = 1, 2, ..., n). \tag{2}$$

On peut résoudre (2) par la formule de Lagrange

$$P(x) = \sum_{1}^{n} y_i L_i(x), \tag{3}$$

où les fonctions fondamentales

$$L_i(x) = \prod_{\substack{j=1 \\ j \neq i}}^{n} \frac{x - x_j}{x_i - x_j}$$

sont telles qu'elles satisfont les équations

$$L_i(x_j) = \delta_{ij}, \quad (i, j = 1, ..., n). \tag{4}$$

Ici, les δ_{ij}, appelés deltas de Kronecker, sont définis par

$$\delta_{i,j} = \begin{cases} 1 & \text{si } i = j \\ 0 & \text{si } i \neq j \end{cases} \tag{5}$$

Pour résoudre le P.R.C., supposons que l'on procède de façon similaire, en considérant les a_i comme des analogues des y_i, et en définissant les entiers b_i tels que

$$b_i \equiv \delta_{ij} \pmod{m_j}, \quad (i, j = 1, ..., n) \tag{6}$$

comme des analogues des fonctions $L_i(x)$. Cela amène au

Théorème 1. *Une solution du système (1) est donnée par*

$$x = \sum_{1}^{n} a_i b_i. \tag{7}$$

En effet, puisque les b_i satisfont (6), on trouve à partir de (7) que

$$x = \sum_{1}^{n} a_i b_i \equiv \sum_{i=1}^{n} a_i \delta_{ij} \equiv a_j \pmod{m_j} \text{ pour tout } \ j = 1, ..., n.$$

Exemple 1. Pour trouver x satisfaisant

$$x \equiv 2 \pmod 5, \quad x \equiv 6 \pmod 7, \quad x \equiv 5 \pmod{11}. \tag{8}$$

On doit résoudre (6) qui dans notre cas est

$$\begin{array}{lll} b_1 \equiv 1 \pmod 5, & b_1 \equiv 0 \pmod 7, & b_1 \equiv 0 \pmod{11}, \\ b_2 \equiv 0 \pmod 5, & b_2 \equiv 1 \pmod 7, & b_2 \equiv 0 \pmod{11}, \\ b_3 \equiv 0 \pmod 5, & b_3 \equiv 0 \pmod 7, & b_3 \equiv 1 \pmod{11}, \end{array}$$

dont on obtient que

$$b_1 \equiv 231, \quad b_2 \equiv 330, \quad b_3 \equiv 210$$

Par (7), on trouve que toutes les solutions de (8) sont données par $x \equiv 27 \pmod{385}$, où $385 = 5 \times 7 \times 11$.

La solution (7) du P.R.C. (1) est essentiellement la solution telle qu'elle est donnée par G. E. Andrews dans [1], et par E. Grosswald dans [2], sans mentionner l'analogie avec la formule de Lagrange. Mon collègue Richard Askey me dit que la remarque de Riesz est bien connue des informaticiens, mais apparemment pas des mathématiciens.

En plus d'enregistrer la remarque de Riesz, la contribution de l'auteur est la remarque suivante : Newton résout le problème de l'interpolation (2) en utilisant des différences divisées successives c_i pour obtenir

$$P(x) = c_1 + c_2(x - x_1) + c_3(x - x_1)(x - x_2) + \ldots + c_n(x - x_1)(x - x_2)\ldots(x - x_{n-1}) \tag{9}$$

où les coefficients c_i sont obtenus en résolvant

$$\begin{cases} y_1 = c_1 \\ y_2 = c_1 + c_2(x_2 - x_1) \\ \vdots \\ y_n = c_1 + c_2(x_n - x_1) + c_3(x_n - x_1)(x_n - x_2) + \ldots + c_n(x_n - x_1)(x_n - x_2)\ldots(x_n - x_{n-1}). \end{cases} \tag{10}$$

En appliquant l'idée de Newton à la solution du P.R.C. (1), on considère les m_i comme étant les analogues des $x - x_i$ et on cherche à déterminer les entiers d_i $(1 \leq i \leq n)$ à partir du système de

congruences

$$(11)\qquad \begin{cases} d_1 \equiv a_1 \pmod{m_1} \\ d_1 + d_2 m_1 \equiv a_2 \pmod{m_2} \\ d_1 + d_2 m_1 + d_3 m_1 m_2 \equiv a_3 \pmod{m_3} \\ \vdots \\ d_1 + d_2 m_1 + d_3 m_1 m_2 + \ldots + d_n m_1 m_2 \ldots m_{n-1} \equiv a_n \pmod{m_n} \end{cases}$$

De cette façon, on obtient le

Théorème 2. *Une solution du P.R.C. (1) est obtenue comme suit : on détermine d'abord les entiers d_i solutions des congruences (11), et alors une solution de (1) est donnée par*

$$(12)\qquad x = d_1 + d_2 m_1 + d_3 m_1 m_2 + \ldots + d_n m_1 m_2 \ldots m_{n-1}.$$

En effet, notons que par (11), les x donnés par (12), satisfont toutes les congruences (1) : pour tout k, $1 \leq k \leq n$, à partir de (12), on obtient que

$$x \equiv d_1 + d_2 m_1 + \ldots + d_k m_1 m_2 \ldots m_{k-1} \pmod{m_k}$$

et par conséquent, par la $k^{\text{ième}}$ congruence (11), on a que $x \equiv a_k \pmod{m_k}$.

Exemple 2. Résolvons le P.R.C. (8) par l'approche de Newton. Pour (8), on a $n = 3, a_1 = 2, a_2 = 6, a_3 = 5, m_1 = 5, m_2 = 7, m_3 = 11$. Comme on peut toujours choisir $d_1 = a_1 = 2$, les $n - 1 = 2$ congruences restantes (11) sont

$$\begin{aligned} 2 + 5d_2 &\equiv 6 \pmod{7}, \\ 2 + 5d_2 + 35d_3 &\equiv 5 \pmod{11}. \end{aligned}$$

La première a comme solution $d_2 = 5$ et la seconde devient maintenant $2 + 25 + 35d_3 \equiv 5 \pmod{11}$ dont la solution est $d_3 \equiv 0 \pmod{11}$. De (12), pour $n = 3$, on obtient que $x = 27$ est une solution de (8).

Une conséquence du théorème 1, ou du théorème 2, est le

Corollaire 1. *Le problème des restes chinois (1) a toujours une solution unique x, mod M, où $M = m_1 m_2 \ldots m_n$.*

De plus, l'un comme l'autre des deux théorèmes fournit une méthode pour trouver cette solution unique.

Gardons fixés les n modules deux à deux premiers entre eux $m_1, m_2, \ldots, m_n$. Combien de problèmes des restes chinois (1) leur correspond-il ? Évidemment, leur nombre est M et on peut contraindre les a_i à prendre les valeurs d'un système de congruences mod m_i, par exemple

$$(13)\qquad a_1 = 0, 1, ..., m_i - 1 \quad (i = 1, ..., n)$$

Pour chaque choix du n-uplet $(a_1, a_2, \ldots, a_n)$, il correspond une unique solution x de (1) qui prend l'une des valeurs

$$x \in \{0, 1, ., M-1\} \quad (M = m_1, m_2, \ldots, m_n). \tag{14}$$

Corollaire 2. *Il y a une correspondance bi-univoque entre les n-uplets $(a_1, \ldots, a_n)$, vérifiant (13), et les M valeurs possible (14) de x.*

Car si deux n-uplets distincts

$$(a_1, a_2, \ldots, a_n) \neq (a'_1, a'_2, \ldots, a'_n) \tag{15}$$

amenaient à rendre égaux x et x' : $x = x'$, on obtiendrait à partir de (1) que

$$a_i \equiv a'_i \pmod{m_i}, \quad (i = 1, ..., n)$$

ce qui contredit notre supposition (15).

Exemple 3. Choisissons l'exemple le plus simple possible : soient $n = 2, m_1 = 2, m_2 = 3$, alors $M = 6$. Ici, par (13), on peut choisir $a_1 = 0, 1$ et $a_2 = 0, 1, 2$. En notant x_r les solutions des 6 P.R.C., on trouve que ces P.R.C. sont

$$\begin{array}{lll} (a) \quad x_1 \equiv 0 \pmod 2 & (b) \quad x_2 \equiv 0 \pmod 2 & (c) \quad x_3 \equiv 0 \pmod 2 \\ \quad\quad x_1 \equiv 0 \pmod 3 & \quad\quad x_2 \equiv 1 \pmod 3 & \quad\quad x_3 \equiv 2 \pmod 3 \\ (d) \quad x_4 \equiv 1 \pmod 2 & (e) \quad x_5 \equiv 1 \pmod 2 & (f) \quad x_6 \equiv 1 \pmod 2 \\ \quad\quad x_4 \equiv 0 \pmod 3 & \quad\quad x_5 \equiv 1 \pmod 3 & \quad\quad x_6 \equiv 2 \pmod 3 \end{array} \tag{16}$$

Leurs solutions se trouvent facilement :

$$x_1 = 0, x_2 = 4, x_3 = 2, x_4 = 3, x_5 = 1, x_6 = 5,$$

qui en effet respecte un système de congruences modulo $M = 6$.

Nous souhaitons terminer notre note avec une application élémentaire de l'application bijective dont il est question dans le Corollaire 2. Pour cela, on a besoin du

Corollaire 3. *Dans le problème des restes chinois (1), on a*

$$(a_i, m_i) = 1 \text{ pour tout } i = 1, ..., n \tag{18}$$

si et seulement si pour la solution x de (1), on a

$$(x, m_1 m_2 \ldots m_n) = 1. \tag{19}$$

En effet, par (1), on voit que (18) est respecté ssi $(x, m_i) = 1$ pour tout i, ce qui est équivalent à (19).

Comme d'habitude, on dénote par $\varphi(m)$ la fonction indicatrice d'Euler qui donne le nombre de nombres positifs $\leq m$ qui sont premiers à m. L'application que nous avons en tête est le

Corollaire 4. *Pour les nombres premiers l'un à l'autre m_i, on a*

$$\varphi(m_1 m_2 \dots m_n) = \varphi(m_1)\varphi(m_2)\dots\varphi(m_n). \tag{20}$$

avec le côté gauche qui est égal au nombre de solutions x de (1) satisfaisant (19), alors que le côté droit donne le nombre de problème des restes chinois satisfaisant les conditions (18).

Exemple 4. Pour les modules $m_1 = 2$ et $m_2 = 3$ de l'exemple 3, seuls les problèmes des restes chinois (e) et (f) satisfont les conditions (18). Notons également que leurs solutions $x_5 = 1$ et $x_6 = 5$ forment effectivement un système réduit de restes mod 6 comme ils doivent le faire.

Remarques. 1. La seconde approche de Newton est légèrement différente et plus économique que la première approche : alors que la première approche nécessite de déterminer les n entiers $b_i \quad (i = 1, 2, ..., n)$, la seconde approche nécessite seulement de trouver les $n - 1$ entiers $d_i \quad (i = 2, 3, ..., n)$.

2. Je dois à Gerald Goodman la référence [3] dans laquelle Ulrich Oberst montre que des formulations abstraites appropriées du problème des restes chinois peuvent devenir la base de beaucoup d'algèbre moderne incluant les principaux théorèmes de la théorie de Galois.

3. Mon collègue Stephen C. Kleene m'informe que Kurt Gödel utilise la solution du problème des restes chinois (en omettant son nom) dans son article fondamental "*Sur les propositions indécidables des Principia Mathematica et sur les systèmes qui leur sont reliés*" dans [4], 145-195, particulièrement dans le lemme 1 de la page 135. Voir aussi la note de bas de page i de la page 136.

4. Originellement, j'ai écrit cette note très brièvement, et même laconiquement. Je dois à l'éditeur une version expansée de cette note et j'ai trouvé très utile de la mettre sous la forme actuelle.

5. Dans un article suivant le présent article, on montrera comment appliquer le théorème des restes chinois pour obtenir des indices pour les modules qui n'admettent pas de racines primitives. Ces indices seront des vecteurs.

Références

[1] G. E. Andrews, Number Theory, W. B. Saunders Co., Philadelphie, 1971.

[2] Emil Grosswald, Topics from the Theory of Numbers, The Macmillan Co., New York, 1966.

[3] Ulrich Oberst, Anwendungen des chinesischen Restsatzes, Expositiones Mathematicae, vol. 3, 1985, 97-148.

[4] Kurt Gödel, Collected Works, volume 1, Oxford University Press, New York, 1986.

[5] I. J. Schoenberg, On the theory and practice of indices mod m, à paraître.