Université Paris 7 – Denis Diderot
U.F.R. de Mathématiques
D.E.U.G. Mathématiques : MT 282

2 novembre 1996

B. Keller

La pratique du lemme chinois

1. Systèmes de congruences

On cherche à résoudre le système

$$\begin{aligned} x &\equiv a_1\ (n_1) \\ x &\equiv a_2\ (n_2) \\ x &\equiv a_3\ (n_3) \end{aligned}$$

où x, les a_i et les n_i sont des entiers (relatifs) et les n_i sont premiers entre eux deux à deux.

Première étape. On cherche des entiers x_1, x_2, x_3 tels que

$$\begin{array}{lll} x_1 \equiv 1\ (n_1) & x_2 \equiv 0\ (n_1) & x_3 \equiv 0\ (n_1) \\ x_1 \equiv 0\ (n_2) \quad ; & x_2 \equiv 1\ (n_2) \quad ; & x_3 \equiv 0\ (n_2) \\ x_1 \equiv 0\ (n_3) & x_2 \equiv 0\ (n_3) & x_3 \equiv 1\ (n_3). \end{array}$$

Pour trouver x_1, on détermine une solution $(u_1, v_1) \in \mathbf{Z}^2$ de l'équation de Bézout

$$n_2\, n_3\, u_1 + n_1\, v_1 = 1$$

Puisque $\mathrm{PGCD}\,(n_2\, n_3, n_1) = 1$, une telle solution existe. On voit que $x_1 = n_2\, n_3\, u_1$ convient. De même, pour trouver x_2 et x_3, on cherche des solutions de

$$\begin{aligned} n_1\, n_3\, u_2 + n_2\, v_2 &= 1 \\ n_1\, n_2\, u_3 + n_3\, v_3 &= 1. \end{aligned}$$

Alors $x_2 = n_1\, n_3\, u_2$ et $x_3 = n_1\, n_2\, u_3$ conviennent.

Seconde étape. La solution générale du système est

$$x \equiv a_1\, x_1 + a_2\, x_2 + a_3\, x_3 \quad (n_1\, n_2\, n_3)\ ,$$

ou, sous une forme plus agréable,

$$\boxed{x \equiv r \quad (n_1\, n_2\, n_3)}$$

où r est le reste de la division euclidienne de $a_1x_1 + a_2x_2 + a_3x_3$ par $n_1n_2n_3$.

Exemple. On cherche à résoudre le système

$$\begin{aligned} x &\equiv 1\ (7) \\ x &\equiv 4\ (9) \\ x &\equiv 3\ (5) \end{aligned}$$

Première étape. Les équations et leurs solutions particulières sont

$$\begin{array}{llll} 45\,u_1 + 7\,v_1 = 1; & \text{sol. part.} & 45 \times (-2) + 7 \times 13 = 1. & \text{Donc} \quad x_1 = -90. \\ 35\,u_2 + 9\,v_2 = 1; & \text{sol. part.} & 35 \times (-1) + 9 \times 4 = 1. & \text{Donc} \quad x_2 = -35. \\ 63\,u_3 + 5\,v_3 = 1; & \text{sol. part.} & 63 \times 2 - 5 \times 25 = 1 & \text{Donc} \quad x_3 = 126. \end{array}$$

Seconde étape. On a

$$a_1\,x_1 + a_2\,x_2 + a_3\,x_3 = 1 \times (-90) + 4 \times (-35) + 3 \times 126 = 148.$$

Ainsi, la solution générale du système est

$$\boxed{x \equiv 148 \quad (315).}$$

2. Isomorphisme d'anneaux

Nous continuons à utiliser les notations et hypothèses du paragraphe ci-dessus. Nous cherchons à expliciter l'inverse ψ de l'isomorphisme canonique

$$\begin{array}{rcl} \phi : \mathbf{Z}/(n_1\,n_2\,n_3) & \tilde{\to} & \mathbf{Z}/n_1 \times \mathbf{Z}/n_2 \times \mathbf{Z}/n_3 \\ {}^{n_1 n_2 n_3}\overline{x} & \mapsto & ({}^{n_1}\overline{x},\ {}^{n_2}\overline{x},\ {}^{n_3}\overline{x}). \end{array}$$

Pour cela, on détermine des entiers x_1, x_2, x_3 comme ci-dessus. Notons que les conditions imposées sur les x_i sont équivalentes aux équations

$$\begin{array}{rcl} \phi\,(\overline{x_1}) & = & (\overline{1}, \overline{0}, \overline{0}) \\ \phi\,(\overline{x_2}) & = & (\overline{0}, \overline{1}, \overline{0}) \\ \phi\,(\overline{x_3}) & = & (\overline{0}, \overline{0}, \overline{1}). \end{array}$$

L'inverse $\psi : \mathbf{Z}/n_1 \times \mathbf{Z}/n_2 \times \mathbf{Z}/n_3 \to \mathbf{Z}/(n_1 n_2 n_3)$ est donné par

$$\psi(\overline{a_1}, \overline{a_2}, \overline{a_3}) = {}^{n_1 n_2 n_3}\overline{a_1 x_1 + a_2 x_2 + a_3 x_3}.$$

3. Remarques

a) Cette méthode s'adapte, avec des modifications évidentes, au cas de 2, 4, 5 ou plus de congruences (resp. facteurs).

b) Une autre méthode consiste à procéder par récurrence sur le nombre de congruences. Dans le cas de trois congruences, par exemple, il n'y a que deux équations de Bézout à résoudre si on utilise cette méthode.