Université Paris Descartes
UFR de Mathématiques et Informatique
45, rue des Saints-Pères 75270 Paris cedex 06

UNIVERSITÉ PARIS DESCARTES

MASTER MA-IM 2011–2012

Logiciels mathématiques

Projet

À remettre : le fichier des fonctions Scilab, le fichier TeX et le fichier compilé au format PDF (ne pas oublier vos noms dans les fichiers source ".sce", ".sci" et ".tex").

Problème

On veut résoudre un système d'équations de congruences linéaires :

$$a_i x \equiv b_i \mod c_i \text{ pour } 1 \leq i \leq N \qquad (SC)$$

où $a_i, b_i, c_i \in \mathbb{N}^*$ $(1 \leq i \leq N)$.

Exemple 1 : le système $x \equiv 2 \mod 3$, $x \equiv 3 \mod 5$, $x \equiv 2 \mod 7$, a comme solution $x = 23 \mod 105$.

Exemple 2 : le système $x \equiv 0 \mod 3$, $x \equiv 1 \mod 6$, n'a pas de solution.

Le *théorème du reste chinois* affirme que le système (SC) a une solution $x \mod m$, où $m = c_1 c_2 \cdots c_N$, si les c_i, $(1 \leq i \leq N)$, sont deux à deux premiers entre, c'est-à-dire $\text{pgcd}(c_i, c_j) = 1$, $(1 \leq i \neq j \leq N)$ et si $\text{pgcd}(a_i, c_i) = 1$, $(1 \leq i \leq N)$.

Algorithme :

(a) calculer $m = c_1 \cdots c_N$;

(b) calculer $q_i = c_1 c_2 \cdots c_{i-1} c_{i+1} \cdots c_N$, $1 \leq i \leq N$;

(c) résoudre les équations $(a_i q_i) r_i \equiv 1 \mod c_i$, $1 \leq i \leq N$;

(d) poser $x_i = q_i r_i$, $1 \leq i \leq N$, alors $x = \sum_{i=1}^{N} b_i x_i \mod m$.

Partie calculs et programmation

1. Écrire la fonction Scilab `function [x,m]=theoreme_chinois(a,b,c)` qui calcule la solution (modulo m) de l'équation (SC) (on prendra garde à vérifier les hypothèses du théorème).
   Cette fonction, ainsi que toute fonction nécessaire par ailleurs, se trouvera dans le fichier `mon_nom_projet.sci`.

2. Dans le fichier `mon_nom_projet.sce` il y aura des exemples d'applications qui font appel à la fonction `theoreme_chinois()`.

Partie rédaction

Le fichier de rédaction comportera les sections suivantes :

3. Description de l'algorithme, des choix de programmation (boucles, pas de boucles, ...).

4. Illustrer avec la solution des problèmes (*cf.* wikipedia) :
   - Le problème du général chinois :
     Après une bataille féroce, le général réunit ses soldats survivants afin de connaître la force de ses troupes précisément. Par un coup d'oeil, il sait qu'il n'a pas plus de 20.000 soldats. Le général ordonne à ses hommes de s'aligner dans plusieurs formations. Ce qui l'intéresse est le nombre de soldats qui restent dehors dans chaque formation. Quand tous les soldats s'alignent à 5 par rangée, il y a 3 soldats qui restent ; à 7 par rangée, il en reste 5 ; 9 par rangée laisse 6 soldats ; par 11 il reste 5 et s'il y a 13 soldats par rangée, 3 restent.
     Par le théorème du reste chinois, le général détermine exactement le nombre de soldats restants.

   - Une bande de 17 pirates possède un trésor constitué de pièces d'or d'égale valeur. Ils projettent de se les partager également, et de donner le reste au cuisinier chinois. Celui-ci recevrait alors 3 pièces. Mais les pirates se querellent, et six d'entre eux sont tués. Un nouveau partage donnerait au cuisinier 4 pièces. Dans un naufrage ultérieur, seuls le trésor, six pirates et le cuisinier sont sauvés, et le partage donnerait alors 5 pièces d'or à ce dernier.
     Quelle est la fortune minimale que peut espérer le cuisinier s'il décide d'empoisonner le reste des pirates ?

5. Pensez à rédiger, illustrer, des commentaires, une introduction,...
   Complétez éventuellement avec d'autres applications de cet algorithme ou des éléments de démonstration du théorème.