UE MODEL – Master d'Informatique
Exercices – Semaine 1

September 28, 2012

1 Exercices simples

Exercices calculatoires (Euclide étendu). Exécuter l'algorithme d'Euclide étendu sur les couples d'entiers suivants:

- $(6, 4)$, $(12, 9)$ et $(32, 16)$
- $(7, 5)$, $(8, 7)$ et $(14, 9)$

Exercices calculatoires (Théorème des restes chinois). Résoudre les équations aux congruences suivantes:

- $X \bmod 5 = 2$ et $X \bmod 7 = 4$
- $X \bmod 4 = 1$ et $X \bmod 7 = 3$
- $X = 1 \bmod 2$, $X = 2 \bmod 3$ et $X = 3 \bmod 5$.
- $X = 1 \bmod 2$, $X = 1 \bmod 3$ et $X = 2 \bmod 5$.

Vous prendrez soin de vérifier chacune de vos solutions. Vous illustrerez aussi que si X_1 et X_2 sont solutions d'une équation aux congruences alors $X_1 - X_2$ est divisible par le produit des modulo.

2 Exercices moins simples

Algorithme de reconstruction (Théorème des restes chinois).

1. À partir de la formule donnée en cours, écrire l'algorithme de reconstruction par théorème des restes chinois.
   Vous privilégierez l'utilisation de la syntaxe Maple.
2. Faites une analyse de complexité de cet algorithme.

3. On s'intéresse à l'algorithme ci-dessous:
   Entrées : des entiers $P_1, \ldots, P_k$ premiers deux à deux et des entiers $A_1, \ldots, A_k$.
   Sortie : Un entier X tel que $X = A_1 \bmod P_1, \ldots, X = A_k \bmod P_k$

   (a) $P \leftarrow P_1$ et $X \leftarrow X_1$
   (b) Pour i allant de 2 à k faire
      i. Calculer u et v tels que $uP_i + vP = 1$ (par Euclide étendu)
      ii. $X \leftarrow uP_iX + vPA_i$
      iii. $P \leftarrow PP_i$
      iv. $X \leftarrow X \bmod P$
   (c) retourner X

   Démontrer que cet algorithme est correct (il résout donc le problème de reconstruction chinoise). Faite une analyse de sa complexité.

4. Comparez les deux algorithmes.

5. Pour la conception d'implantations optimisées, lequel des deux algorithmes a votre préférence?

Généralisation de la reconstruction chinoise au cas dégénéré. Le théorème des restes chinois et la reconstruction associée ne s'appliquent que dans les situations où les modules sont premiers deux à deux. Dans cet exercice, nous étudions ce qu'il est possible de faire en levant cette restriction.

Nous allons montrer le résultat suivant. Soit $P_1, \ldots, P_k$ et $A_1, \ldots, A_k$ des entiers. Alors X est solution de

$$\begin{array}{rcl} X & = & A_1 \bmod P_1 \\ & \vdots & \\ X & = & A_k \bmod P_k \end{array} \tag{1}$$

si et seulement si

$$A_i = A_j \bmod \mathsf{GCD}(P_i, P_j)$$

pour tout couple d'entiers i, j choisis dans $\{1, \ldots, k\}$.

1. Démontrer que la condition ci-dessus est nécessaire.

   Pour montrer qu'il s'agit d'une condition suffisante, nous allons exhiber, sous cette condition, une méthode (calculatoire) permettant d'obtenir une solution au problème.

2. Posons $P_0 = \mathsf{PPCM}(P_1, P_2)$ et A_0 tel que $A_i = A_j \bmod \mathsf{GCD}(P_i, P_j)$ pour tout i, j dans $\{0\} \cup \{3, \ldots, k\}$. Démontrer que l'ensemble des solutions de (1) est le même que celui de

$$\begin{array}{rcl} X & = & A_0 \bmod P_0 \\ & \vdots & \\ X & = & A_k \bmod P_k \end{array} \tag{2}$$

Indications: On montrera l'inclusion des ensembles de solutions dans un sens puis dans l'autre. On utilisera intensivement la relation de Bézout ainsi que les propriétés de la division euclidienne.

3. En déduire un algorithme.

Extensions de l'algorithme d'Euclide au cas des polynômes. On considère l'ensemble des polynômes en une variable dans un corps $\mathbb{K}$; il sera noté $\mathbb{K}[X]$.

1. Montrer que doté des opérations d'addition et de multiplication sur les polynômes il s'agit d'un anneau.
2. Écrire les algorithmes d'addition et de multiplication dans $\mathbb{K}[X]$ et faire une analyse de complexité.
3. Généraliser l'algorithme de division euclidienne au cas de couples de polynômes dans $\mathbb{K}[X]$. Faire une analyse de complexité.
4. Généraliser l'algorithme d'Euclide au cas de couples de polynômes dans $\mathbb{K}[X]$. Faire une analyse de complexité.

3 Exercices pour Travaux sur Machines Encadrés

1. Implantez les fonctions donnés sur les transparents de cours (Semaine 1) et exécutez-les.
2. Implantez les algorithmes d'Euclide étendu et de reconstruction chinoise vus en cours et en TD. Vous prendrez soin de vérifier que vos implantations sont correctes (vous pourrez notamment comparer avec les implantations disponibles dans le système Maple).
3. Ëvaluez les performances de vos implantations; jusqu'à quelle taille de données pouvez-vous calculer? Les complexités prouvées en TD vous semblent-elles réalistes au regard des performances des implantations ?