SÉANCE 6. THÉORÈME DE RESTE CHINOIS ET FONCTION INDICATRICE D'EULER

Objectifs : Théorème chinois et fonction indicatrice d'Euler.

Exercice 3 (Théorème des restes chinois) — Rappelons le *théorème des restes chinois* :

> *étant donné un nombre entier $m > 1$ et une factorisation $m = m_1 m_2 \cdots m_r$ en produit d'entiers $m_i > 1$* deux à deux premiers entre eux, *l'application naturelle*
>
> $$f : \mathbf{Z}/m\mathbf{Z} \longrightarrow \mathbf{Z}/m_1\mathbf{Z} \times \mathbf{Z}/m_2\mathbf{Z} \times \cdots \times \mathbf{Z}/m_r\mathbf{Z}$$
>
> $$x \bmod m \longmapsto (x \bmod m_1, x \bmod m_2, \ldots, x \bmod m_r)$$
>
> *est un isomorphisme d'anneaux.*

1. Démontrez que f est bien un isomorphisme d'anneaux.
2. Expliquez comme construire f^{-1}.
3. Soit L une liste de nombres entiers. Écrire un algorithme `Test(L)` vérifiant si les coefficients de L sont deux à deux premiers entre eux.
4. Si $L = [m_1, \ldots, m_r]$ est une liste d'entiers premiers deux à deux premiers entre eux, écrire un algorithme `Chinois(a,L)` calculant, pour tout $a \in \mathbf{Z}$, les composantes de $f(a)$.
5. Considérons toujours une liste $L = [m_1, \ldots, m_r]$ d'entiers premiers entre eux deux à deux et posons $m = m_1 m_2 \cdots m_r$.
   (i) Soit $i_0 \in \{1, \ldots, r\}$. À l'aide d'une identité de Bézout bien choisie, déterminer un entier e_{i_0} tel que
   $$e_{i_0} \equiv 1 \bmod m_{i_0} \quad \text{et} \quad e_{i_0} \equiv 0 \bmod m_i$$
   pour tout $i \neq i_0$.
   (ii) En déduire un algorithme `ChinoisInverse(L,X)` associant à toute liste $X = [a_1, a_2, \ldots, a_r]$ de nombres entiers l'unique entier $a \in \{0, \ldots, m-1\}$ tel que $a \equiv a_i \bmod m_i$ pour tout i.
6. En guise d'application, considérons $m = 100 \cdot 101 \cdot 103$. Déterminer un nombre entier a tel que $a \equiv 60 \bmod 103$ et $\mathrm{pgcd}(a, m) = 1$.

Exercice 4 (La fonction indicatrice d'Euler) — On rappelle que l'indicatrice d'Euler est la fonction φ qui a un entier $n > 0$ associe le nombre d'entiers m compris entre 1 et n et premiers à n.

1. Montrer que φ est une fonction *multiplicative*, c'est-à-dire qu'étant donnés $n, m \geq 1$ premiers entre eux, on a $\varphi(nm) = \varphi(n)\varphi(m)$.

   Indication : Remarquez que pour tout entier $N \geq 1$, $\varphi(N)$ est le cardinal de l'ensemble $(\mathbf{Z}/N\mathbf{Z})^*$ des éléments inversibles de $\mathbf{Z}/N\mathbf{Z}$. Utilisez ensuite le théorème des restes chinois.
2. Soit p un nombre premier et $k \geq 1$ un entier. Calculez $\varphi(p)$ puis justifiez que $\varphi(p^k) = (p-1)p^{k-1}$. Soit n un entier ≥ 1. Déduire une expression de $\varphi(n)/n$ en fonction des facteurs premiers de n.

3. Ecrire une fonction `ListeEntiersPremiers(n)` renvoyant la liste des entiers m compris entre 1 et n et premiers à n.
4. Ecrire une fonction `Phi(n)` renvoyant $\varphi(n)$.
5. Ecrire une version récursive `PhiRecursive(n)` de la fonction précédente. On pourra penser à d'abord écrire une fonction intermédiaire `DecompoPartielle(n)` prenant en argument n et renvoyant (p,k,m), avec p,k,m des entiers ≥ 1 tels que $n = p^k m$ et p ne divisant pas m.
6. Ecrire une fonction `SumPhi(n)` renvoyant $\sum_{d|n}\varphi(d)$. Que peut-on conjecturer sur `SumPhi` ?
7. Soit n un entier ≥ 1. Pour tout diviseur d de n, on note

$$A_d := \{1 \leq k \leq n; k \wedge n = d\}.$$

Montrez que A_d est l'ensemble des k s'écrivant $d \times \ell$ avec ℓ un entier compris entre 1 et n/d premier à n/d. En déduire le cardinal de A_d, puis que

$$\sum_{d|n} \varphi(d) = n.$$

8. En utilisant la formule de la question précédente, écrire une version récursive `PhiRecursive2(n)` calculant $\varphi(n)$.
9. Tracez l'ensemble des $\varphi(n)/n$ pour n compris entre 1 et 100.
10. Trouvez une suite $(a_n)_{n\geq 1}$ d'entiers telle que $\varphi(a_n)/a_n$ tende vers 1 lorsque n tend vers l'infini.
11. (Difficile) On note $(p_i)_{i\geq 1}$ la suite des nombres premiers ordonnés par ordre croissant et on définit $b_k = p_1 \cdots p_k$ pour tout $k \in \mathbf{N}$. Montrez que $\varphi(b_n)/b_n$ tend vers 0 lorsque n tend vers l'infini.

Indication : En remarquant que $1/(1-1/p) = \sum_{k\geq 0} 1/p^k$, justifiez que

$$\prod_{p \text{ premiers}} \frac{1}{1-1/p} = \sum_{n\geq 1} \frac{1}{n} = +\infty.$$