Programmation Effective – TD 06 : Jeux mathématiques

matthieu.gallet@ens-lyon.fr

mardi 11 mars 2008

1 La fonction ϕ d'Euler

Également connue sous le nom d'indicatrice d'Euler, ϕ est définie de $\mathbb{N}^*$ dans $\mathbb{N}$ et associe à tout entier n le nombre d'entiers positifs inférieurs à n et premiers avec lui. Ainsi, on a $\phi(8) = 4$, car 8 est premier avec 1, 3, 5 et 7.

1.1 Calcul de ϕ

La valeur de l'indicatrice d'Euler s'obtient par l'expression de n donnée par le théorème fondamental de l'arithmétique : Si $n = \prod_{i=1}^{q} p_i^{k_i}$, alors on a

$$\phi(n) = \prod_{i=1}^{q} (p_i - 1)\, p_i^{k_i - 1} = n \prod_i (1 - \frac{1}{p_i}).$$

Dans la formule, p_i désigne un nombre premier et k_i un entier strictement positif. En effet, le caractère multiplicatif de l'indicatrice d'Euler et une récurrence montre que :

$$\phi(n) = \prod_{i=1}^{q} \phi(p_i^{k_i})$$

Il suffit alors de dénombrer le nombre d'entiers non premiers avec une puissance d'un nombre premier et plus petit que celui-ci pour remarquer que :

$$\forall i \in [1, q], \phi(p_i^{k_i}) = p_i^{k_i} - p_i^{k_i - 1} = (p_i - 1) p_i^{k_i - 1}$$

Ce qui permet de conclure la démonstration.

1.2 Propriétés

L'indicatrice d'Euler est une fonction essentielle de l'arithmétique modulaire, elle est à la base de résultats fondamentaux, à la fois en mathématiques pures et appliquées. Un entier p est premier si et seulement si $\phi(p) = p - 1$. Cette propriété est une conséquence directe du calcul explicite de l'indicatrice. La cryptologie utilise largement cette fonction. Le code RSA se fonde sur le théorème d'Euler, indiquant que si n est un entier strictement positif et a un entier premier avec n, alors $a^{\phi(n)} = 1 (mod n)$. On dispose également de l'égalité suivante :

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

La somme et le produit sont étendus à tous les diviseurs positifs d de n.

$\phi(n)$ est égal au nombre de générateurs d'un groupe cyclique d'ordre n et à l'ordre du groupe des unités de l'anneau $\mathbb{Z}/n\mathbb{Z}$ (le groupe des unités désigne l'ensemble des éléments inversibles pour la multiplication de l'anneau). ϕ est multiplicative : si u et v sont deux entiers strictement positifs et premiers entre eux, alors $\phi(uv) = \phi(u)\phi(v)$ (conséquence du théorème des restes chinois).

Croissance de ϕ Asymptotiquement, nous avons $n^{1-\varepsilon} < \phi(n) < n$ pour n'importe quel ε et $n > N(\varepsilon)$. En fait, si nous considérons $\frac{\phi(n)}{n}$, nous pouvons écrire, à partir de la formule précédente, sous forme de produit de facteurs $1 - p^{-1}$, où les p sont des nombres premiers divisant n. Par conséquent les valeurs de n correspondantes aux valeurs particulièrement petites du rapport sont les n qui sont le produit d'un segment initial de la suite de tous les nombres premiers. À partir du théorème des nombres premiers il peut être montré qu'une constante ε dans la formule précédente peut par conséquent être remplacée par $C\frac{\log\log n}{\log n}$.

Quelques autres formules

$$\phi(n^m) = n^{m-1}\phi(n), \text{ pour } m \geq 1$$

$$\sum_{1 \leq k \leq n, (k,n)=1} k = \frac{1}{2} n\phi(n), \text{ pour } n > 1$$

$$\sum_{k=1}^{n} \frac{k}{\phi(k)} = \mathcal{O}(n)$$

$$\sum_{k=1}^{n} \frac{1}{\phi(k)} = \mathcal{O}(\log(n))$$

2 Applications

Résolvez les problèmes suivants : `http://acm.uva.es/p/v102/10299.html`, `http://acm.uva.es/p/v112/11254.html`,`http://acm.uva.es/p/v111/11179.html`,`http://acm.uva.es/p/v109/10929.html`, `http://acm.uva.es/p/v108/10885.html`,`http://acm.uva.es/p/v108/10871.html`.