DS d'informatique
Nombres premiers, nombres composés

Durée : 2 heures

28 mai 2011

L'utilisation des calculatrices n'est pas autorisé.

Le problème porte sur les nombres premiers et composés. Il va de soi que l'utilisation de la fonction Maple `isprime` est interdite.

Les deux parties sont indépendantes et peuvent être traitées séparément.

On rappelle qu'un nombre entier $n > 1$ est dit *premier* si ses seuls diviseurs sont 1 et n. Dans le cas contraire il est dit *composé*. Le PGCD de deux entiers a et b sera noté (a, b). On rappelle que la fonction Maple pour calculer le PCGD de `a,b` est `gcd(a,b)`.

1 Tests de composition

Le but de cette partie est d'obtenir des algorithmes rapides pour déterminer si un nombre est composé, mais dont l'échec ne prouve pas nécessairement la primalité du nombre testé.

1. On veut construire un test de composition à l'aide du théorème suivant :

   Théorème 1. *Soit $N, a \in \mathbb{Z}$. Si N est premier et $(a, N) = 1$, alors on a*

   $$a^{N-1} = 1 \pmod{N}.$$

   a) Sans utiliser la puissance de Maple, écrire une procédure `Puissance` qui prend en argument des entiers a, q, N et qui renvoie $a^q \bmod N$.

   b) Écrire une procédure `TestFermat` qui prend en argument deux entiers a, N et qui renvoie `true` si le théorème précédent permet de prouver que N est composé, et `false` sinon.

2. Le test précédent n'est pas bon car il échoue à détecter certains nombres qui ne sont pas premiers, par exemple 561. Il peut être raffiné à l'aide d'un outil sophistiqué : le symbole de Jacobi. Nous n'étudierons pas le symbole de Jacobi mais nous en donnerons quelques propriétés, suffisantes pour calculer sa valeur. Le symbole de Jacobi $\mathrm{J}(M, N) \in \{-1, 0, 1\}$ est défini pour tout couple d'entiers M, N avec $N > 1$ impair, et vérifie :

   i) pour tout $k \in \mathbb{Z}$, $\mathrm{J}(M + kN, N) = \mathrm{J}(M, N)$;

   ii) pour tout $a, b \in \mathbb{Z}$, $\mathrm{J}(ab, N) = \mathrm{J}(a, N)\,\mathrm{J}(b, N)$;

   iii) $\mathrm{J}(0, N) = 0$;

   iv) $\mathrm{J}(1, N) = 1$;

   v) $\mathrm{J}(-1, N) = (-1)^{\frac{N-1}{2}}$;

   vi) $\mathrm{J}(2, N) = (-1)^{\frac{N^2-1}{8}}$;

vii) si $M > 1$ est impair, alors $\mathrm{J}(M,N) = (-1)^{\frac{(M-1)(N-1)}{4}}\,\mathrm{J}(N,M)$.

On a alors le théorème suivant

Théorème 2. *Soit $N, a \in \mathbb{Z}$. Si N est premier impair, alors on a*

$$a^{\frac{N-1}{2}} = \mathrm{J}(a,N) \pmod{N}.$$

a) En admettant que $13^{280} = 1 \pmod{561}$, effectuer à la main le test du théorème 2 avec $a = 13$ et $N = 561$. On indiquera soigneusement les propriétés utilisées pour calculer le symbole de Jacobi.

b) Écrire une procédure `Jacobi` qui prend en argument deux entiers M, N avec N impair et qui renvoie $\mathrm{J}(M,N)$. Justifier soigneusement la validité de la procédure. *Indication : on pourra chercher une méthode analogue à l'algorithme d'Euclide pour le calcul du PGCD.*

c) Écrire une procédure `TestSolovayStrassen` qui prend en argument deux entiers a, N et qui renvoie `true` si le théorème précédent permet de prouver que N est composé, et `false` sinon.

2 Tables de nombres premiers

Le but de cette partie est d'obtenir la liste de tous les nombres premiers inférieurs à une borne donnée.

1. On va commencer par utiliser un test élémentaire de primalité.
   a) Écrire une procédure `EstPremier` qui prend en argument un entier N et qui renvoie `true` ou `false` suivant que N est premier ou non, en appliquant la définition.
   b) On peut montrer facilement que si un nombre N est composé, alors il admet un diviseur inférieur ou égal à $\sqrt{N}$. En utilisant cette observation, écrire une nouvelle procédure `EstPremier2` qui fait la même chose que la précédente mais plus rapidement.
   c) Écrire une procédure `TablePremiers` qui prend en argument un entier B et qui renvoie la liste des nombres premiers inférieurs ou égaux à B, en testant la primalité de chaque entier.
2. On va maintenant utiliser la technique du crible d'Ératosthène, plus efficace. Elle consiste à commencer par écrire tous les nombres de 2 à une borne B dans un tableau. On raye tous les multiples de 2. Le nombre suivant non rayé (3) est premier. On raye tous ses multiples. Le nombre suivant non rayé est premier, on raye ses multiples, etc.
   Écrire une procédure `TablePremiers2` qui fait la même chose que `TablePremiers`, mais en utilisant la méthode du crible d'Ératosthène.
3. Évaluer le nombre d'opérations élémentaires (affectation, comparaison, opération arithmétique, etc) effectuées par les procédures `TablePremiers` et `TablePremiers2`. On admettra la formule

$$\sum_{p \leq X} \frac{1}{p} = O(\log\log X)$$

où la somme porte sur les nombres premiers inférieurs ou égaux à X.