Université Claude Bernard, Ens Lyon 2001-2002
Magistère Math-Info, Calcul formel, TD du 28 septembre 2001

Exercice 1 : Construire un grand nombre premier

De nombreux algorithmes en cryptographie, dont le plus connu est RSA, nécessitent l'utilisation de grands nombres premiers (de l'ordre de la centaine de chiffres décimaux). On se propose ici de construire de tels nombres en utilisant le théorème de Lucas.

1. Écrire la procedure Maple
   `> start := proc(n)`
   qui reçoit l'entier n, et rend un nombre M produit de premiers consécutifs (quoique que cette consécutivité soit tout à fait secondaire) plus grand que 10^n.

2. Ecrire la fonction booléenne
   `> lucas := proc(P,a)`
   qui reçoit P et a et qui rend vrai si et seulement si P est premier et a un générateur du groupe multiplicatif de $\mathbb{Z}/P\mathbb{Z}$.

3. Ecrire enfin la fonction
   `> bigprime(n)`
   qui rend un nombre premier supérieur à 10^n.

4. **Application** : donner un nombre premier de plus de 200 chiffres. Vérifiez que le nombre premier obtenu est premier en utilisant le test probabiliste prédéfini `isprime` de Maple. Bien sûr, la fonction `nextprime` de Maple, permet d'obtenir plus rapidement un grand nombre probablement premier, en pratique certainement premier. L'application du théorème de Lucas vous donne un nombre garanti premier.

Exercice 2 : Calcul, par crible d'un tableau de valeurs consécutives de la fonction μ de Möbius.

Vous pouvez programmer cet exercice en Maple si vous le souhaitez, mais vous obtiendrez un programme beaucoup plus rapide en programmant en C, ou Pascal, ou Fortran ....

1. Commencez par programmer le crible d'Eratosthène de l'intervalle $[1..N]$. Quel est le temps de calcul (on admettra l'équivalence, au voisnage de l'infini,

$$\sum_{p \leq x} \frac{1}{p} \sim \log\log x$$

où x est un réel plus grand que 1, et la sommation porte sur les nombres premiers $p \leq x$) ?

2. Modifiez le programme précédent, de sorte qu'il rende toutes les valeurs de la fonction de Möbius sur l'intervalle $[1..N]$, en s'inspirant des indications suivantes : Dans le crible d'Eratosthène le tableau de crible est un tableau de booléens, initialisés à vrai, et, pour supprimer l'entier n, on affecte la valeur faux à la n^{eme} case du tableau. Ici le tableau de crible est un tableau d'entiers, μ indexé par $[1..N]$. La case $\mu[n]$ est initialisée avec n. Tout entier n plus grand que 1, est candidat à être premier tant que $\mu[n] = n$. Quand on crible par le nombre premier p, au lieu de mettre à faux la case pk, dont le numéro est multiple de p, on divise son contenu par $-p$.

3. **Application** : Soit $S(n)$ la somme partielle d'ordre n

$$S(n) = \sum_{k=1}^{n} \frac{\mu(k)}{k}.$$

Donnez les valeurs $S(10)$, $S(100)$, $S(1000)$, $S(10000)$, $S(100000)$, $S(1000000)$ et émettez une conjecture.

Exercice 3 : Minoration de $\varphi(n)$

Soit $n \geq 2$, $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$.

1. En minorant $\left(1 - \frac{1}{p_j}\right)$ par $\left(1 - \frac{1}{j+1}\right)$ dans l'équation

$$\frac{\varphi(n)}{n} = \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_k}\right)$$

montrer que

$$\frac{\varphi(n)}{n} \geq \frac{1}{k+1}.$$

2. En déduire que

$$\varphi(n) \geq n \frac{\log 2}{2 \log n}.$$

Exercice 4

Soit a un entier impair non divisible par 5. Montrer qu'il existe un multiple entier de a dont l'écriture décimale ne contient que des 9.

Montrer qu'il existe aussi un multiple entier de a dont l'écriture de comporte que des 1.