Tests de primalité

Le but de cet exercice est de comprendre comment tester la primalité d'un entier. Avant de s'attaquer au problème, on lira attentivement la page d'aide «mod (modulo)» de Maple» et on s'attachera à comprendre ce que fait l'expression `i &^ n mod m` qui y est décrite.

1. Étudier le programme suivant et comprendre ce qu'il est censé faire et pourquoi il est incorrect. Le corriger.

```
estpremier := proc(n)
  local i;
  if n=2 then return true; fi;
  if n<=1 then return false; fi;
  if irem(n,2) = 0 then return false; fi;
  i := 3;
  while i*i < n and irem(n,i) <> 0 do
    # ici n n'est pas divisible par i ni par aucun nombre impair
    # inférieur à i, ni par deux.
    # on essaie le suivant
    i := i + 2;
  od;
  if i*i < n then return false; else return true; fi;
end;
```

2. Essayez de trouver un entier premier n aussi grand que possible de façon à ce que Maple mette moins de 10s à tester sa primalité avec le programme corrigé.

3. Le but est de trouver une méthode plus efficace pour tester la primalité d'un entier. On s'intéressera ici au test de Fermat. Soit n un entier. On sait que si n est premier, alors pour tout entier $a \in]0, n[$, on a $a^{n-1} \equiv 1[n]$. Donc par contraposée, si $a^{n-1} \not\equiv 1[n]$, alors n n'est pas premier. On dit alors que a est un témoin de non-primalité du test de Fermat pour n. Si $a^{n-1} \equiv 1[n]$ mais que n n'est pas premier, on dit que n est un pseudo-premier de Fermat de base a.

   Y a t-il des entiers compris entre 1 et 1000 qui soient des pseudo-premiers de Fermat de base 2 (on les appelle aussi nombres de Poulet) ? Lesquels ?

   Y a t-il des entiers n compris entre 1 et 1000 qui soient des pseudo-premiers de Fermat de base a pour tout a ? Pour presque tous ?

4. Le logiciel de chiffrement PGP utilise des tests de Fermat (avec les bases 2, 3, 5 et 7) pour trouver un nombre premier.[1] Essayez d'avoir une idée de la taille du plus grand nombre que vous puissiez trouver avec ce test de façon à ce que Maple mette moins de 10s à tester la primalité d'un entier. Jusqu'à combien pouvez-vous aller ?

5. On propose maintenant un autre test, appelé test de Miller-Rabin. Il fonctionne de la façon suivante. Pour tester si un entier n est premier, on commence par écrire $n-1$ sous la forme $2^s \times m$, où m est impair. Soit $a \in [\![1, n-1]\!]$. Le test repose sur le résultat suivant : si n est premier, alors ou bien $a^m \equiv 1[n]$, ou bien il existe $d \in [\![0, s-1]\!]$ vérifiant $a^{2^d \cdot m} \equiv -1[n]$. On peut démontrer ce

[1] Le risque de choisir accidentellement un nombre non-premier est apparemment très faible pour les plages de nombres testées par PGP.

résultat en utilisant le petit théorème de Fermat, le fait que si n est premier $\mathbb{Z}/n\mathbb{Z}$ est un corps et le fait que dans tout anneau intègre, l'équation $x^2 = 1$ a au plus deux solutions[2] (1 et -1).

On dira que a est un menteur fort s'il vérifie les conditions ci-dessus et que n n'est pas premier.

On peut montrer qu'au plus un quart des valeurs de $[\![1, n-1]\!]$ sont des menteurs forts.[3] Le test de Miller-Rabin s'effectue donc en pratique de la façon suivante : prendre une valeur a au hasard comprise entre 1 et $n-1$ et effectuer le test avec cette base a. Si a respecte les conditions données ci-dessus, n est probablement premier, dans ce cas, on recommence avec un nouveau a pris au hasard. Si au bout de 40 essais, on n'a pas trouvé de a violant les conditions données plus haut, on considérera que le nombre donné était premier.

Pour effectuer le test aussi vite que possible, on calcule a^m dans $\mathbb{Z}/n\mathbb{Z}$ et on effectue ensuite des mises au carré successives pour calculer a^{2m}, a^{4m},...,$a^{2^{s-1}m}$. De plus, on n'est pas obligé de calculer toutes ces valeurs : on s'arrête dès le début si $a^m \equiv 1[n]$, on s'arrête également dès qu'on trouve la valeur -1, et enfin on peut aussi s'arrêter si l'on trouve la valeur 1 (pourquoi ?).

Mettre en œuvre ce test pour vérifier si les grands nombres que vous avez trouvés avec le test de Fermat sont bien premiers.

[2] Dans certains anneaux intègres, il n'y en a qu'une, par exemple dans $\mathbb{Z}/2\mathbb{Z}$, où $-1 = 1$.

[3] Voir sur Wikipédia en anglais l'article *Miller–Rabin primality test* et notamment Schoof, René, *Four primality testing algorithms*, Algorithmic Number Theory: Lattices, Number Fields, Curves and Cryptography, Cambridge University Press, ISBN 0521808545, http://tinyurl.com/schoof-miller-rabin.