TP n^o 4 : Arithmétique et applications

Serge Dupont (2004)

L'objectif de ce TP est d'apprendre à utiliser Maple pour résoudre des problèmes d'Arithmétique, mais aussi de découvrir ses applications modernes.

1 Prise en main.

1.1 Question

Lire l'aide et prévoir ce que va répondre Maple à :

```
> ?mod:
> mods(8,9): modp(8,9):
```

1.2 Question

Comparer en temps de calcul

```
> 123456789^987654 mod 4 ; 123456789&^987654 mod 4;
```

2 Critères de primalité.

Un nombre entier > 1 est dit composé s'il n'est pas premier. On s'intéresse à la question : tel nombre est-il composé ? On va construire des tests pour cette propriété, qui seront plus efficaces que le crible d'Erathostène.

2.1 Critère d'Erathostène

Critère 1 *Un nombre n est premier si et seulement si il n'admet aucun diviseur p tel que* $1 < p \leq \sqrt{n}$.

2.1.1 Question

Ecrire un programme **Eratho** qui renvoie *true* si *n* est premier et *false* sinon. Le tester sur les entiers de la forme $n! + 1$. $20! + 1$ est-il premier ?

2.2 Critère de Fermat

Critère 2 *Un entier n est composé si et seulement si il existe un entier a,* $1 < a < n$ *tel que* a^{n-1} *n'est pas congru à 1 modulo n.*

C'est une conséquence du petit théorème de Fermat. Remarquer que ce critère teste si *n* est composé, pas premier. Un *a* qui permet de prouver par le critère 2 que *n* n'est pas premier s'appelle un *témoin de Fermat* (de non-primalité).

2.2.1 Question

Ecrire un programme **Fermat(n,a)** qui renvoie *true* si *a* est un témoin de Fermat (et donc *n* n'est pas premier) et *false* sinon (et on ne sait pas si *n* est premier ou composé). Vérifier que 2 est un témoin de Fermat (de non-primalité) pour tous les entiers composés plus petits que 100. (Il y a plusieurs manières de faire. Utiliser la commande *isprime*)

2.2.2 Question

Quel est le plus petit nombre composé pour lequel $a = 2$ n'est pas un témoin de Fermat ? Quels sont les nombres composés ≤ 10000 pour lesquels 2 n'est pas un témoin de Fermat ?

2.2.3 Question

Prouver avec ce critère que $20!+1$ n'est pas premier.

2.2.4 Question

Quel est le plus petit entier pour lequel ni $a=2$, ni $a=3$ ne sont des témoins de Fermat ? Et ni 2,3,5 ? Ni 2,3,5,7 ? En déduire un critère rapide pour tester si un nombre ≤ 25000 est premier (on ne demande pas de l'écrire).

2.3 Critère de Miller-Rabin

Critère 3 (Miller-Rabin) *Soit n un entier impair. Ecrivons $n-1=t\,2^s$ avec t impair. Supposons qu'il existe un entier a strictement compris entre 1 et n tel que a^t ne soit pas congru à 1 modulo n et $a^{(t\,2^j)}$ ne soit pas congru à -1 modulo n pour tout j compris entre 0 et $s-1$. Alors n est composé.*

Un tel entier a est appelé un *témoin de Miller* pour n. Le critère précédent est à la base d'un test *probabiliste* de primalité. L'idée est de tirer des a au hasard et regarder si ce sont des témoins de Miller. Si l'un en est un, on est sûr que n est composé. Si aucun n'en est un, alors on peut espérer que n est premier. On n'en est pas sûr, mais la probabilité d'échec est faible, parce la proportion de témoins de Miller est forte pour les nombres composés : plus de 75% ! Voir à ce propos la dernière question.

On pourra utiliser la fonction **isprime** de Maple pour évaluer les performance de la méthode.

2.3.1 Question

Ecrire un programme *decomp* affichant la liste $[s,t]$ ou s et t sont les entiers intervenant dans la décomposition de $n-1$.

2.3.2 Question

Ecrire un programme *Rabin* testant si un entier a compris entre 1 et n est un témoin de Miller pour n. Remarquer que n est un entier impair. (Répondre a si a est un témoin et 0 sinon.) L'appliquer à des exemples intéressants issus des questions ci-dessus.

2.3.3 Question

Ecrire ensuite un programme **estpremierprob** tirant au hasard 20 nombres entre 1 et n et affichant "composé" si un des entiers tiré est un témoin de Miller et "premier" sinon. (En fait, comme on l'a dit, au moins les trois quarts des entiers compris entre 1 et n sont des témoins de Miller, si n est composé bien sûr. La probabilité que ce test affiche "premier" pour un nombre qui ne l'est pas est inférieure à 10^{-6}. On peut encore faire chuter cette probabilité en augmentant le nombre de tirage.) Utiliser la fonction **rand**. (Voir l'aide.)

2.3.4 Question

Sauriez-vous trouver un nombre composé dont 2 n'est pas un témoin de Miller ?

2.3.5 Question

Sauriez-vous trouver le plus petit entier composé dont ni 2 ni 3 ne sont des témoins de Miller ?

2.3.6 Question

En fonction de l'entier impair n, afficher sur un graphique le pourcentage d'entiers compris entre 2 et $n-1$ qui sont des témoins de Miller pour n, n entier impair composé variant de 3 à 1001. On mettra en abscisse les entiers composés et en ordonnées le pourcentage de témoins de Miller.

2.3.7 Question

Tester si les entiers de Fermat $2^{(2^k)}+1$ et de Mersenne 2^k-1 sont premiers pour des petites valeurs de k.