

TP3 : Tests de primalité

N'oubliez pas d'exécuter (valider avec la touche Entrée) les commandes Maple (texte en rouge) avant de les utiliser.

On sait que si m est un nombre premier alors $a^{(m-1)} \bmod m = 1$ pour a entre 1 et $m-1$ (Fermat), donc si on trouve un a entre 1 et $m-1$ tel que $a^{(m-1)} \bmod m \neq 1$ on peut en déduire que m n'est pas un nombre premier. Quelle chance ce test a-t-il de réussir pour des a pris au hasard ? C'est ce que nous allons expérimenter.

– Les fonctions ou opérateurs de Maple dont vous aurez besoin

Le très bon test de primalité de Maple. On lui fera confiance.

```
[ > isprime(561576002580391);  
[ > isprime(561576002580401);
```

Le calcul de puissance modulaire se fait avec l'opérateur $\&\wedge$ qui réduit par le modulo en cours de calcul de la puissance ce que ne fait pas l'opérateur usuel \wedge .

```
[ > 416545^456454 mod 4545445;  
[ > 416545&^456454 mod 4545445;
```

– Test utilisant la relation de Fermat

Exercice 1 : On dit qu'un nombre m est a -pseudopremier, si m n'est pas un nombre premier mais $a^{(m-1)} \bmod m = 1$ et donc le test rate. Ecrire une fonction qui rende **true** si m est a -pseudopremier **false** sinon (vous pouvez utiliser **isprime**).

Exercice 2 : En utilisant cette fonction construire les listes des nombres 2-pseudopremiers, 3-pseudopremiers et 5-pseudopremiers inférieurs à 1200 (vous pouvez utiliser **select**). Que déduisez-vous de la comparaison de ces trois listes ?

Exercice 3 : Les nombres 561 et 1105 résistent mieux que les autres aux tests : ils apparaissent dans deux des trois listes. Montrer qu'ils vérifient la propriété suivante : $a^{(m-1)} \bmod m = 1$ pour tout a premier avec m . Ce sont des nombres de Carmichael.

Exercice 4 : En prenant a au hasard entre 1 et $m-1$ quelle chance a-t-on de détecter que 561 n'est pas premier ? Même question pour 1105.

Nous allons améliorer ce test avec la méthode de Miller vue en cours : on veut tester si m (impair) est un nombre premier. On pose $m-1 = 2^s t$ avec t impair. On calcule la suite

$a_0 = a^t \bmod m, a_1 = a^{(2^1 t)} \bmod m, \dots, a_s = a^{(2^s t)} \bmod m$. Si $a_s \neq 1$ ou s'il existe un i tel que $a_i = 1$ et $a_{i-1} \neq 1$ et $a_{i-1} \neq -1$ alors m n'est pas un nombre premier.

– Test amélioré (Miller)

Exercice 5 : Ecrire une fonction qui rende **false** si m satisfait ce test pour le nombre a , **true** sinon.

Exercice 6 : En utilisant cette fonction construire comme dans l'exercice 2 des listes de nombres qui résistent à ce test (vous pouvez agrandir l'intervalle testé).

Exercice 7 : Les nombres 561 et 1105 résistent-ils à ce test ?