Premiers Algorithmes pour reconnaître si p est premier : Algorithme 1

1. On divise p par tous les entiers compris entre 2 et $p-1$ (inclus)
2. Dès qu'un entier divise p on arrête la boucle car p n'est pas premier

Ecrire une fonction estPremier(p) en Python

Algorithme 2

Améliorer l'algorithme 1 après avoir démontré la proposition suivante :

Si p est *composé*, c'est à dire il existe b et c entiers tel que $a = bc$ alors l'un des deux nombres b ou c est inférieur ou égal à $\sqrt{p}$ la racine carrée de p

Algorithme 3

Améliorer l'algorithme 2 en divisant p uniquement par les nombres premiers inférieurs à $\sqrt{p}$

Algorithme 4 : Crible d'Eratosthène

1. Pour connaître tous les nombres premiers jusqu'à n
2. On part de la liste des entiers de 2 jusqu'à n
   Enlever tous les multiples de 2 sauf 2
3. Passer au nombre plus grand que 2 encore présent c'est à dire 3 et enlever tous les multiples de 3 sauf 3
4. etc... s'arrêter lorsqu'on atteint la racine carrée de n
5. Ce qui reste est la table des nombres premiers jusqu'à n

Faire une fonction cribleEratosthene(n)

Test de Fermat On rappelle le petit théorème de Fermat :

Si p est premier et ne divise pas a alors $a^{p-1} \equiv 1[p]$

Par conséquent par contraposition si $a^{p-1} \neq 1[p]$ alors p n'est pas premier

1. Vérifier que $n = 21$ n'est pas premier en prenant $a = 2$
2. Pour le calcul de a^{p-1} on verra en TP un algorithme plus efficace, l'algorithme d'exponentiation modulaire rapide
3. Attention ! $2^{340} \equiv 1[341]$ et pourtant 341 est composé car $341 = 11 \times 31$. On dit alors que 341 est **2-pseudo premier**
4. Que vaut $3^{340}[341]$?

Test probabiliste de primalité de Fermat :

1. Choisir au hasard un nombre a au hasard entre 2 et $p-1$
2. Si $a^{p-1} \equiv 1[p]$ alors déclarer que p est premier

Nombres de Carmichael Il existe des nombres n composés a-pseudo premiers qui mettent en défaut le test de Fermat pour tout a premier avec n. Ils sont appelés les nombres de Carmichael . Il n'y en a que 7 jusqu'à 10000 et 16 jusqu'à 100 000.

Le plus petit nombre de Carmichael est $561 = 3 \times 11 \times 17$

Tester $a^{560}[561]$ pour a premier avec $561 = 3 \times 11 \times 17$