Théorème des nombres premier : (+preuve)

# Méthode déterministe

Choix d’un nombre aléatoire de taille .

Test des entiers inferieurs à comme diviseurs de .

Si aucun entier divise , alors est premier.

Complexité :

# Méthode probabiliste

Test de Miller-Rabin

Choix d’un nombre aléatoire de taille .

Effectuer k test de Miller-Rabin.

Si tout les tests sont bons, alors p est pseudo-premier ; sinon, on choisit un nouveau p aléatoire.

Complexité :

Détail du test :

Probabilité (+ preuve)