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

Complexité :

Détail théorique du test :

Si p est premier alors Z/pZ est un corps (résultat du cours qui s’obtient avec le théorème de Bezout).

On s’intéresse à l’équation dans Z/pZ. Comme c’est un corps, c’est en particulier un anneau intègre. En factorisant l’équation ci-dessus sous la forme :

On s’aperçoit que les seules solutions de cette équation, par intégrité, sont 1 et -1. (1)

On prend premier.

On écrit sous la forme :   (s est le nombre maximal de fois que l’on peut mettre 2 en facteur dans ).

Soit (appelé témoin de Miller) dans Z/pZ, on pose la suite avec : .

Par le petit théorème de Fermat, on sait que. On montre grace à (1) que si il existe tel que n’est pas congru a 1 modulo alors il existe un indice i∈{k,…,s−1} tel que : .(2)

En effet, posons . Un tel nombre existe car n’est pas congru a 1 modulo (l'ensemble que l'on considère est non vide), et pour tout  (l'ensemble est majoré par). Ainsi, on a . D'autre part . D'après (1),  ou . La première possibilité est exclue par définition de . Donc

Le test de Miller-Rabbin consiste à calculer la suite des pour voir si elle vérifie bien (2). On dit que passe le test si les satisfont effectivement (2). Si ne passe pas le test alors on est sûr que n’est pas premier sinon on ne peut rien dire. Il reste à itérer ce processus avec plusieurs témoins de Miller, l’heuristique du système étant « plus passe de tests plus il a de chance d’être premier ». L’efficacité de ce test vient du fait que le nombre de témoin « menteur », c’est-à-dire les témoins qui permettent à de passer le test alors qu’il n’est effectivement pas premier, est inférieur à du nombre d’entiers inférieurs à .

Probabilité (+ preuve)