Tarea Automatizada #1

Marco Teórico

Jhon Sebastian Rojas Rodriguez

Test de primalidad de Miller-Rabin

El test de primalidad de Miller-Rabin es un algoritmo para determinar si un número es primo, similar al test de primalidad de Fermat. Fue propuesto como un algoritmo determinista por Gary Lee Miller basándose en la hipótesis de Rieman, la cual no está demostrada. Michael Oser Rabin con la propuesta de Miller obtuvo un algoritmo probabilistico que no utiliza la hipótesis.

Las propiedades de los primos que dan lugar al algoritmo son el pequeño teorema de Fermat:

(1) $$si\ p\ es\ primo, entonces\ a^{p-1} \equiv 1 (mod\ p)$$

y la propiedad:

(2) $$si\ p\ es\ primo\ y\ algún\ a \in \mathbb{Z}\ satisface\ a^2 \equiv 1 (mod\ p), entonces\ a \equiv \pm 1 (mod\ p)$$

El test asegura que n no es primo cuando no satisface una de estas dos propiedades, en caso contrario lo cataloga como un “probable primo”. Es el test más utilizado en la práctica debido a la baja probabilidad de fallo, la cual esta dada por el número de iteraciones que se realice el algoritmo con una base a escogida al azar: la probabilidad de que un número compuesto pase la prueba en h iteraciones es $\frac{1}{4^h}$.

La especificación completa del algoritmo se encuentra en el PDF de diseño de la aplicación.

Bibliografia:

Miller, Gary (1975). «Riemann's Hypothesis and tests for primality». *Journal of Computer and System Sciences*: 300-317

Rabin, Michael (1980). «Probabilistic algorithm for testing primality». *Journal of Number Theory*: 128-138.

Ben Lynn (Stanford University) Mathematics and Computer Science Notes: Number theory. Primality Tests. https://crypto.stanford.edu/pbc/notes/numbertheory/millerrabin.html

Test de primalidad de Miller-Rabin:

https://es.wikipedia.org/wiki/Test_de_primalidad_de_Miller-Rabin