Licenciatura en ciencia de la computación

Algoritmo p-1 de Pollard

Matemática Computacional

Profesor:
Nicolas Thériault

Autor:
Sergio Salinas
Danilo Abellá

Contents

1 Introducción

El informe trata sobre el analisis del los tiempos de ejecución del algoritmo p-1 de Pollard, para implementarlo se uso el lenguage C junto con la librería GMP en su versión 6.

2 Formulación experimentos

Se probo el resultado con los tres números pedidos, pero para que el tiempo sea más exacto se ejecuto el algoritmo por durante un minuto y se calculo el primedio, los resultados son los siguientes.

n	B	Tiempo
28742705413	9973	0.003851
45524252104894451218081	107	0.000052
176506841202696015718206304213347...	655	0.009753

Los datos dan indicios que el tiempo de ejecución depende más del valor que alcance B que del tamaño del número, para estar más seguros de esto se ejecuto el programa mil veces con valores al azar que van desde el 2 al 1000000000000 y se hicieron dos gráficos, uno que compara el tiempo vs B y otro que compara tiempo vs Número.

Para que el tiempo sea más preciso se repetitio cada ejecución por durante el lapso de un 1 segundo y se calculo un promedio entre todos los tiempos.

Se uso una función del gmp que calculaba la probabilidad de que un número sea primo, a la hora generar números al azar para crear la gráfica, se usaba esta función para saber si el número resultante era posiblemente primo, si lo era se descartaba y se probaba otro. Esta función no fue agregada al tiempo de ejecución del algoritmo.

La tabla resultante de puede ver en en informe/DATOS.txt, la primera columna es el número probado, la segunda el valor de B alcanzado y la tercera el tiempo de ejecución.

3 Información de Hardware y Software

3.1 Notebook - Danilo Abellá

3.1.1 Software

- SO: Xubuntu 16.04.1 LTS
- GMP Library
- Mousepad 0.4.0

3.1.2 Hardware

- AMD Turion(tm) X2 Dual-Core Mobile RM-72 2.10GHz
- Memoria (RAM): 4,00 GB(3,75 GB utilizable)
- Adaptador de pantalla: ATI Raedon HD 3200 Graphics

3.2 Notebook - Sergio Salinas

3.2.1 Software

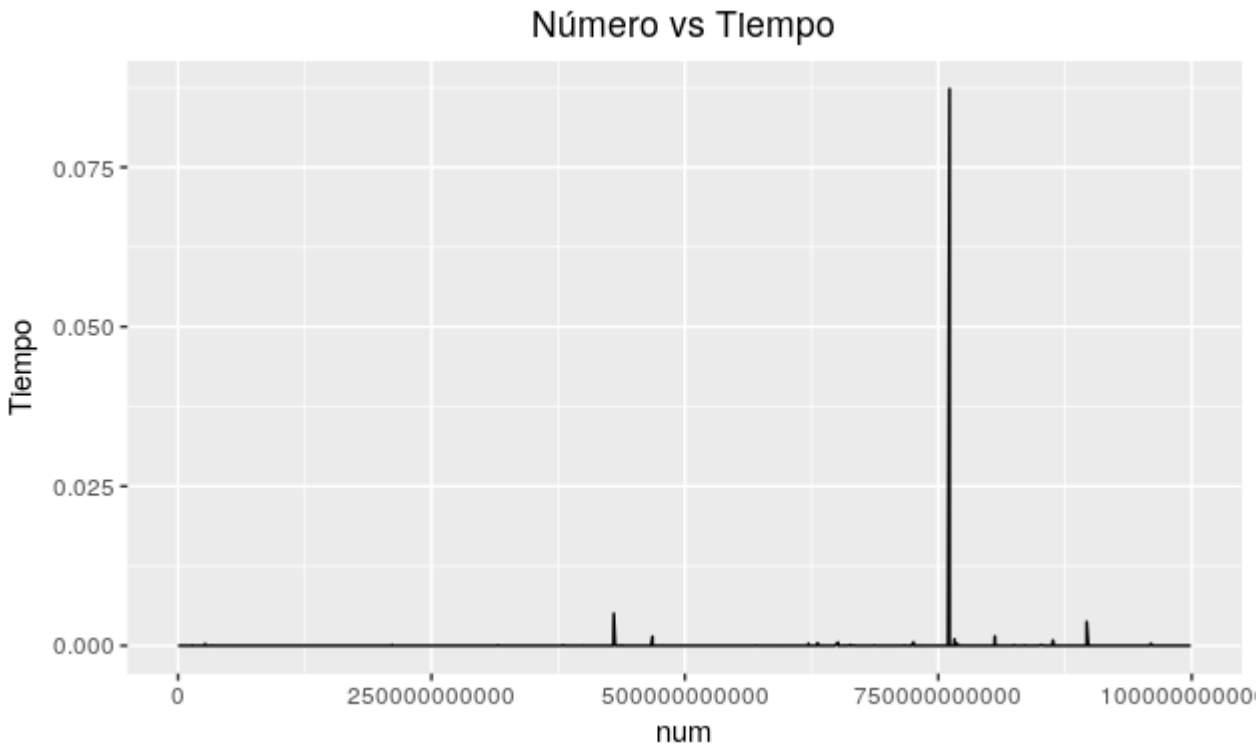
- SO: ubuntu Gnome 16.04 LTS
- Compilador: gcc version 5.4.0 20160609
- Editor de text: Atom

3.2.2 Hardware

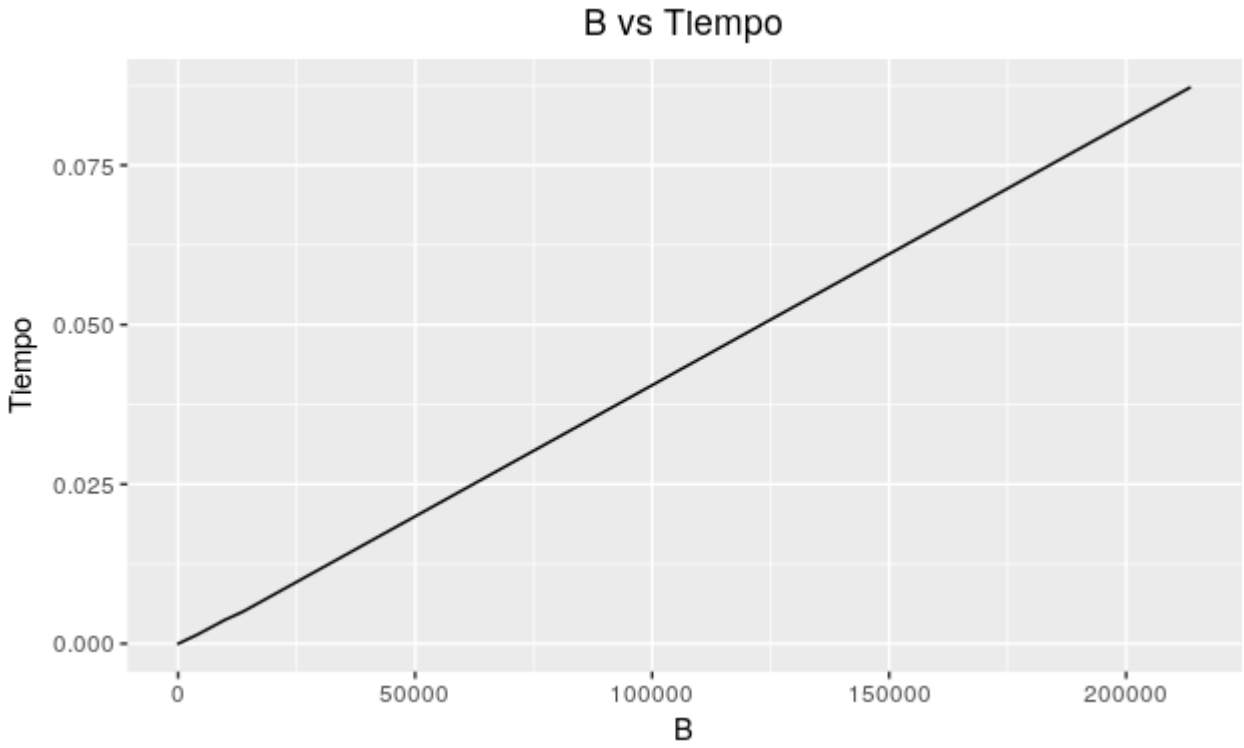
- Procesador: Intel Core i7-6500U CPU 2.50GHz x 4
- Video: Intel HD Graphics 520 (Skylake GT2)

4 Curvas de desempeño de resultados

4.1 Número vs Tiempo



4.2 B vs Tiempo



5 Conclusiones

Con los primeros valores probados y en las gráficas queda claro que el tiempo se ejecución se mantiene constante independiente del tamaño del número, pero a medida que B va creciendo también lo va haciendo el tiempo, el caso más estremo fue el visto con el número 761126431349 que se demoro 0.087253s y alcanzo un valor B de 213623, mientras que el resto de los números que tenían valores B menores a 5 su tiempo de ejecución era de 0.000001s.