Cryptography

Diego Alfonso Prieto Torres - Sebastian Camilo Martinez Reyes

14 de noviembre de 2012

Índice

1. Contextualizacion

El problema de Brave Balloonist es un problema usado en maratones de programacion cuyo enunciado puede encontrarse actualmente en el Juez en Linea TIMUS identificado con el codigo 1049. Este es un problema que esta clasificado dentro de la teoria de numeros, y por lo tanto, es la oportunidad perfecta para desafiar los conocimientos matematicos, combinados con las habilidades en programacion. El documento describe la estrategia que se uso para dar una solucion eficiente y asi el estudiante se desarrolle en los contextos de programacion y matematicos de forma fluida.

1.1. Objetivos

- Encontrar la cantidad de divisores positivos de un numero entero positivo que es mayor que 1.
- Encontrar varias estrategias apoyadas en la teoria de numeros para que la solucion del ejercicio sea mas eficiente y tarde menos del limite que se estipula.
- Implementar la estrategia mas eficiente y visualizar como la teoria de numero de mano con la programacion es una herramienta muy poderosa en la solucion de problemas.

1.2. Precondicion

Como precondicion reciviremos 10 numeros enteros, todos ellos dentro del intervalo $[1, 10000]$.

1.3. Poscondicion

Lo que nuestro programa debe lograr informar es un numero N que representa el ultimo digito de la cantidad de divisores del producto de los 10 numeros dados inicialmente.

2. Definicion del Problema

2.1. Definicion de Conceptos

Se entiende por divisor de un numero entero b, un numero entero a tal que el modulo es igual a 0. La notacion que se usara para indicar que a es divisor de b, o leido textualmente a divide a b sera la siguente :

$$a \ddagger b \equiv true$$

Los divisores de un numero r es el conjunto S de todos los enteros positivos tales que :

$$S = \{i : int \mid 1 \leq i \leq r \wedge i \ddagger r : i\}$$

La cantidad de divisores de un numero r no es mas que la cardinalidad del conjunto S. Asi que si entendemos M como el numero de divisores de r obtenemos:

$$M = \#S$$

2.2. Introduccion al Problema

Como visualizamos a simple vista, podria resultar un problema muy sencillo, ya que bastaria solamente con encontrar los divisores de un numero; pero lo realmente complicado es cuando ese numero es muy grande y la solucion se torna demorada en ejecucion, para ello nos podemos apoyar en una estrategia, que mas que eso es un teorema matematico que soluciona el problema de una manera eficiente.

3. Modelamiento de la Solucion

3.1. Estrategia de la Solucion

La cantidad de divisores que tiene un numero puede hallarse de dos formas, siendo la mas sensilla a nuestro modo de ver esta:

Se obtiene sumando 1 a todos los exponentes de los factores primos del numero, y multiplicando los resultados obtenidos.

El numero 72 descompuesto en sus factores primos es: $112 = 2^4 * 7^1$
Por lo tanto la cantidad de divisores M que posee el numero 72 es:

$M = (4 + 1) * (1 + 1)$
$M = 5 * 2$
$M = 10$

Ahora como la respuesta al ejercicio debe ser el ultimo digito del numero, solo basta con obtener el modulo 10 de M y el ejercicio estara resuelto.

3.2. Leve Nocion de Estructura de Datos

Se recomienda, un poceso iterativo, y una estructura de datos que les permita almacenar el exponente del factor primo.

4. Conclusiones

Reincistimos en que la teoria de numeros es un arma poderosisima en la solucion de problemas de este tipo, ya que la matematica, lo que logra con estos teoremas que nos ofrece, es evitar que el programador haga recorridos exahustivos, reduce la complejdad de su algoritmia analisando el problema de formas que quizas nunca se le hubiesen ocurrido al programador como metodologia de la solucion, por otro lado, esto no se puede lograr sin una investigacion del tema y sin sensibilidad para hallar el mejor de los muchos teoremas que se ofrecen, claro, teniendo en claro el conexto del problema.