Algorithms for Problem Solving – 11650

Teoría de Números

Jon Ander Gómez Adrián
jon@dsic.upv.es

Departament de Sistemes Informàtics i Computació
Escola Tècnica Superior d'Enginyeria Informàtica
Universitat Politècnica de València

25 de febrero de 2014

Factorización

- *factorización* o *descomposición en factores primos* de enteros.
- *multiplicidad*: lo que distingue la factorización de 4 de la de 8.
- Existen $n/\ln n$ primos en $[1 \ldots n]$.
- La Criba de Eratóstenes es la manera más eficiente para completar la lista de primos hasta n.
- *divisibilidad*: los divisores un número n son 1 y todas las combinaciones de sus factores primos.

MCD

- El algoritmo más eficiente es el de Euclides. Veamos su versión en la que nos devuelve los factores x e y tal que

$$a \cdot x + b \cdot y = mcd(a, b)$$

al aplicar la recursión

$$b \cdot x' + a' \cdot y' = mcd(a, b)$$

sustituyendo a' por su valor $a \texttt{ mod } b$

$$b \cdot x' + (a - b \cdot \lfloor a/b \rfloor) \cdot y' = mcd(a, b)$$

- $mcm(a, b) = (a * b)/mcd(a, b)$

- La aritmética modular permite trabajar con números grandes utilizando enteros de 32 o 64 bits.
- Suma:

$$(x + y) \texttt{ mod } n = ((x \texttt{ mod } n) + (y \texttt{ mod } n)) \texttt{ mod } n$$

- Resta:

$$(x - y) \texttt{ mod } n = (n + (x \texttt{ mod } n) - (y \texttt{ mod } n)) \texttt{ mod } n$$

- Producto:

$$(x * y) \texttt{ mod } n = ((x \texttt{ mod } n) * (y \texttt{ mod } n)) \texttt{ mod } n$$

- Potencias

$$(x^y) \bmod n = (x \bmod n)^y \bmod n$$

- ¿Cuál es el último dígito de 2^{100}?

$2^3 \bmod 10 = 8$

$2^6 \bmod 10 = (8 * 8) \bmod 10 = 4$

$2^{12} \bmod 10 = (4 * 4) \bmod 10 = 6$

$2^{24} \bmod 10 = (6 * 6) \bmod 10 = 6$

$2^{48} \bmod 10 = (6 * 6) \bmod 10 = 6$

$2^{96} \bmod 10 = (6 * 6) \bmod 10 = 6$

$2^{100} \bmod 10 = (2^{96} * 2^3 * 2^1) \bmod 10 = (6 * 8 * 2) \bmod 10 = 6$

- $a \equiv b (\texttt{mod}\ m)$ equivale a decir que m es divisor de $(a - b)$.
- ¿Qué enteros x satisfacen $x \equiv 3 (\texttt{mod}\ 9)$?
- ¿Qué enteros x satisfacen $2x \equiv 3 (\texttt{mod}\ 9)$?
- ¿Qué enteros x satisfacen $2x \equiv 3 (\texttt{mod}\ 4)$?

- Suma y resta:

$$a \equiv b(\texttt{mod}\ n) + c \equiv d(\texttt{mod}\ n) = a + c \equiv b + d(\texttt{mod}\ n)$$

- Producto:

$$(a \equiv b(\texttt{mod}\ n)) * (c \equiv d(\texttt{mod}\ n)) = ac \equiv bd(\texttt{mod}\ n)$$

- División:

$$ad \equiv bd(\texttt{mod}\ nd) = a \equiv b(\texttt{mod}\ n)$$

si d es divisor común a a, b y n.

$a \equiv b(\texttt{mod}\ n)$ será falsa si $mcd(a, n)$ no es divisor de b.

110701/10110

- Este problema se puede solucionar con enteros de 32 bits sin signo, no es necesario utilizar números grandes.
- No entraña ninguna dificultad si averiguamos, manualmente y con paciencia, la respuesta (*yes* o *no*) para los 20 o 30 primeros números.
- Así observaréis que no es necesario obtener los divisores de cada número para determinar si quedará apagada o encendida, según si el número de estos es par o impar, respectivamente.

110702/10006

- Se puede precalcular el resultado y almacenarlo en una tabla. Tamaño relativamente pequeño (65000 valores).
- Conviene utilizar la criba de Eratóstenes para determinar los primos hasta 65000.
- Es necesario utilizar aritmética modular para saber si $a^n \bmod n = a$

  Si y es par tenemos: $x^y \bmod n = (((x \bmod n)^{y/2} \bmod n) * ((x \bmod n)^{y/2} \bmod n)) \bmod n$

  si es impar entonces: $x^y \bmod n = (((x \bmod n)^{y/2} \bmod n) * ((x \bmod n)^{y/2} \bmod n) * (x \bmod n)) \bmod n$

110703/10104

- Para este problema tan sólo debemos aplicar el método de Euclides para obtener el máximo común divisor (mcd).
- En concreto la versión del libro que obtiene los valores x e y de la ecuación

$$a \cdot x + b \cdot y = mcd(a, b)$$

- Es posible que los cálculos desborden los enteros de 32 bits. Antes de probar con aritmética de números grandes intentad con enteros de 64 bits por si admite la solución.

110704/10139

- Para que un número n divida al factorial de otro número a, es imprescindible que todos los factores primos de n estén contenidos en todos los números que van del 2 al a, ambos inclusive.
- Por ejemplo, ¿96 divide a $10!$?
- La descomposición en factores primos de 96 es $2^5 \times 3^1$, y

$$10! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10$$

- Como vemos, el 3 aparece en el productorio seis veces: una en el propio 3, dos veces en el 6 y tres en el 9.
- El 2 aparece más de cinco veces, en concreto 8: una en el propio 2, dos en el 4, una en el 6, tres en el 8 y una más en el 10.

110705/10168

- Mediante la criba de Eratóstenes se debe preparar una tabla para saber si un número es primo o no. La tabla sólo necesita un bit por cada número a comprobar.
- Una tabla con todos los primos que necesitamos no cabe en memoria. Se debe implementar una función que compruebe si un número es primo, si es inferior al tamaño de la tabla consultando la tabla, en caso contrario se comprueba por programa.
- Según Goldbach cualquier entero par mayor o igual a 4 se puede expresar como la suma de dos primos.
- La estrategia consiste en buscar el primo más grande inferior a la cuarta parte del número y restárselo.
- Al valor resultante se le resta un primo para que quede como un número par.
- Finalmente buscamos dos primos cuya suma coincida con el valor que queda.
- ¿Para qué números podemos aplicar la estrategia descrita con la seguridad de que encontraremos los 4 primos?

110706/10042

- Buscar el primer valor m mayor que n tal que se cumpla la condición descrita en el enunciado.

  n es el valor de entrada.

- Para ello debemos calcular cada vez:
  - Suma de los dígitos de m.
  - Descomposición en factores primos de m, sumar los dígitos de cada factor y acumularlos.

- Cuando coincidan ambos cálculos ya tenemos un número de Smith.

110707/10090

- Debemos resolver una ecuación del tipo

$$n_1 * x + n_2 * y = N$$

  donde N es el número total de canicas.

- La combinación de x e y debe ser tal que el valor de $c_1 * x + c_2 * y$ sea mínimo.

- ¿Qué valor conviene que sea el máximo posible? ¿x o y?

- Supongamos que nos interesa que x sea el máximo, ¿cómo obtener el valor de x tal que y pueda ser un entero que cumpla la ecuación?

Del tema 7 hemos abordado los problemas:

- 110701/10110 “Light, More Light”
- 110702/10006 “Carmichael Numbers”
- 110703/10104 “Euclid Problem”
- 110704/10139 “Factovisors”
- 110705/10168 “Summation of Four Primes”
- 110706/10042 “Smith Numbers”
- 110707/10090 “Marbles”