

1. La siguiente fórmula es bien conocida:

$$\sum_{j=1}^n j^2 = \frac{n(n+1)(2n+1)}{6}.$$

Estima en función de n el número de bit-operaciones necesarias para calcular tanto el término de la izquierda como el de la derecha.

2. Se trata de estimar en función de n el número de bit-operaciones necesarias para calcular el producto de todos los números primos menores que n . Suponemos que hemos calculado con anterioridad una lista muy larga que contiene todos los primos menores que n

a) Si definimos $\pi(n) = \text{Card}\{p \in \mathbf{N} \mid p < n, p \text{ es primo}\}$, el Teorema del Número Primo nos dice que $\lim_{n \rightarrow \infty} \frac{\pi(n)}{n/\log n} = 1$. Utiliza este resultado para estimar el número de dígitos en el producto de todos los números primos menores que n .

b) Da una cota para el número de bit-operaciones necesarias para hacer una de las multiplicaciones que intervienen en dicho producto.

c) Estima el número total de bit-operaciones necesarias para calcular el producto de todos los números primos menores que n .

3. Probar que 15 es un pseudo-primo en base 4, que 28 es un pseudo-primo en base 9 y que 91 es un pseudo-primo en base 3.

4. Sea n un número impar compuesto y sea $(b, n) = 1$.

a) Sea p un divisor primo de n y escribamos $n' = n/p$. Probar que si n es un pseudo-primo en base b entonces $b^{n'-1} \equiv 1 \pmod{p}$.

b) Demostrar que ningún entero de la forma $n = 3p$, con $p > 3$ primo, puede ser un pseudo-primo en bases 2, 5 ni 7.

c) Demostrar que ningún entero de la forma $n = 5p$, con $p > 5$ primo, puede ser un pseudo-primo en bases 2, 3 ni 7.

d) Probar que 91 es el menor pseudo-primo (impar) en base 3.

5. a) Probar que si $2^n - 1$ es primo entonces n es primo, y que si $2^n + 1$ es primo entonces $n = 2^k$. Los números $M_p := 2^p - 1$, con p primo, se llaman “números de Mersenne” y “primos de Mersenne” en caso de ser primos. Los de la forma $F_k := 2^{2^k} + 1$ se llaman “números de Fermat” y “primos de Fermat” si son primos. Los primeros primos de Mersenne son 3, 7, 31, 127, y todos los primos de Fermat conocidos son 3, 5, 17, 257 y 65537.

b) Probar que todos los números de Fermat y todos los números de Mersenne son pseudo-primos en base 2. (SUGERENCIA: Para los números de Fermat, estudiar primero $2^{2^k} \pmod{F_k}$, y comprobar que podemos calcular 2^{F_k} a partir de este valor por iteración de cuadrados. Para los de Mersenne, empezar por ver que $p|M_p - 1$ y deducir de ello que $M_p = 2^p - 1 | 2^{M_p - 1} - 1$.)

c) A pesar de lo anterior, comprobar que uno puede ver que $M_{11} = 2047$ no es primo utilizando un sencillo test de primalidad.

6. a) Prueba que los siguientes son números de Carmichael: 561, 1105, 1729, 2465, 2821, 6601, 41041, 825265.

b) Demuestra que 561 es el menor número de Carmichael.

7. Supongamos que m es un entero positivo tal que $6m + 1$, $12m + 1$ y $18m + 1$ son todos primos. Demostrar que $n = (6m + 1)(12m + 1)(18m + 1)$ es un número de Carmichael. (Esta idea es una de las que han sido utilizadas para intentar demostrar que hay infinitos números de Carmichael, y durante mucho tiempo fue el método utilizado para encontrar números de Carmichael muy grandes.)

8. Dado que es muy fácil saber si un número par es primo o no (el único par primo es el 2), no tiene demasiado sentido aplicar tests de primalidad a los números pares. Sin embargo, y por aquello de tener una teoría completa, se pide: demostrar que no existen números de Carmichael pares, o sea, que para todo n par existe b tal que $(b, n) = 1$ y $b^{n-1} \not\equiv 1 \pmod{n}$.

9. Recordemos que la existencia de infinitos números de Carmichael es un resultado reciente (Alford, Granville, Pomerance 1992). Sin embargo, la existencia de infinitos pseudo-primos (verdaderos, o sea, no primos) en base 2 era bien conocida. Posiblemente la demostración más simple es la siguiente (Malo 1903): probar que si n es un pseudo-primo en base 2 compuesto, entonces $n' := 2^n - 1$ también es un pseudo-primo en base 2 compuesto. (SUGERENCIA: Tanto la composición como la pseudo primalidad se basan en el hecho de que si $a|b$ entonces $2^a - 1|2^b - 1$, y en observar que si n es pseudo-primo en base 2 entonces $n|n' - 1$.)

10. Los números 85026517 y 85026567 son producto de dos primos. Factorizarlos.

11. El número 12871 es el producto de dos primos. Utiliza el método de Kraitchick-Dixon para factorizarlo.