

1. Probar que 15 es un pseudoprimo en base 4, que 28 es un pseudoprimo en base 9 y que 91 es un pseudoprimo en base 3.
2. 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 pseudoprimo 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 pseudoprimo en bases 2, 5 ni 7.
  - c) Demostrar que ningún entero de la forma  $n = 5p$ , con  $p > 5$  primo, puede ser un pseudoprimo en bases 2, 3 ni 7.
  - d) Probar que 91 es el menor pseudoprimo (compuesto) impar en base 3.
3.
  - 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 pseudoprimos 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  $M_p = 2^p - 1 | 2^{M_p - 1} - 1$ .)
4.
  - 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.
5. 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.)
6. 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  $\gcd(b, n) = 1$  y  $b^{n-1} \not\equiv 1 \pmod{n}$ .
7. Recordemos que la existencia de infinitos números de Carmichael es un resultado reciente (Alford, Granville, Pomerance 1992). Sin embargo, la existencia de infinitos pseudoprimos (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 pseudoprimo (compuesto) en base 2, entonces  $n' := 2^n - 1$  también es un pseudoprimo (compuesto) en base 2. (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 pseudoprimo en base 2 entonces  $n|n' - 1$ .)
8. Encontrar todos los primos de Mersenne  $M_p := 2^p - 1$  con  $p < 30$ .
9. Los números 85026517 y 85026567 son producto de dos primos. Factorizarlos.
10. Los números 12871, 2599 y 21449 son producto de dos primos. Utiliza el método de Kraitchick para factorizarlos.

11. Sabemos que el número 340531 es producto de dos primos. Calcular estos primos.
12. Calcula un divisor no trivial de los números 2039189 y 10097063 mediante el método  $p-1$ .
13. Usa el método  $\rho$  de Pollard para factorizar los números 1111 y 1189.
14. Sea  $N \in \mathbb{N}$  compuesto. Demostrar que si conocemos  $x \in \mathbb{Z}/N\mathbb{Z}$  distinto de  $\bar{0}$  y  $\bar{1}$  tal que  $x^2 = x$ , entonces podemos factorizar  $N$  de forma eficiente.
15. Usa el algoritmo Baby-step giant-step para calcular
  - a)  $\log_2 17$  en  $\mathcal{U}(\mathbb{Z}/29\mathbb{Z})$ ,
  - b)  $\log_7 59$  en  $\mathcal{U}(\mathbb{Z}/71\mathbb{Z})$ .