Aritmètica Modular i RSA

1. Calculeu:
   (a) $3^{28} \mod 10$,
   (b) $3^{200} \mod 15$.

2. 2EXP modular. Doneu un algorisme de temps polinòmic que amb entrada els enters a, b, c i un nombre primer p computi $a^{b^c} \mod p$.

3. Factorial Modular. Donats dos enters x i N, calcula $x! \mod N$.
   (a) Demostreu que un enter y es primer si i només si per a tot enter $x < y$ es compleix que $gdc(x!, y) = 1$.
   (b) Considereu l'apartat previ per demostrar que si Factorial Modular fos computable en temps polinòmic, aleshores el problema de Factoritzar també seria computable en temps polinòmic (Recordeu Factoritzar: Donat un nombre enter x, calcula els seus factors primers).

4. En un sistema criptogràfic RSA amb $p = 7$ i $q = 11$, troba la clau pública (N, c) i la clau privada (N, d) apropiades.

5. Sistema criptogràfic segur?. Suposem que en lloc d'utilitzar un nombre compost $N = pq$ com es fa en el sistema RSA, utilitzem un nombre primer p. Per encriptar un missatge $m \mod p$ farem servir un exponent e, de la mateixa manera que es fa en el sistema RSA. L'encriptament del missatge $m \mod p$ seria $m^e \mod p$.

   Demostreu que aquest nou sistema no és segur donant un algorisme eficient per desencriptar. Es a dir, doneu un algorisme que, amb entrada $p, e, m^e \mod p$, computi $m \mod p$ eficientment. Justifica la correctesa de l'algorisme i analitza el seu temps de computació.