# Teoría de Números 2024

Lista 05

27.septiembre.2024

1. Sea $m = pq$ producto de dos primos distintos $p < q$. Hallar una fórmula para $p$ y para $q$ en términos de $m$ y $\varphi(m)$.

   Asumiendo que $m = 39247771$ es producto de dos primos distintos, usar esta fórmula para encontrar $p$ y $q$, sabiendo que $\varphi(m) = 39233944$.

2. Muestre que si $d \mid n$, entonces $\varphi(d) \mid \varphi(n)$.

3. Para cualquier $n \in \mathbb{N}$, sea $\sigma(n)$ la suma de los divisores positivos de $n$; por ejemplo, $\sigma(6) = 1 + 2 + 3 + 6 = 12$ y $\sigma(10) = 1 + 2 + 5 + 10 = 18$.

   Supongamos que $n = pqr$ con $p < q < r$ primos distintos. Diseñe un algoritmo eficiente que, dados $n$, $\varphi(n)$ y $\sigma(n)$, calcule la factorización de $n$. Por ejemplo, si $n = 105$, entonces $p = 3$, $q = 5$ y $r = 7$, por lo que la entrada al algoritmo sería $n = 105$; $\varphi(n) = 48$ y $\sigma(n) = 192$; y la salida sería $3$, $5$ y $7$.

   Con su algoritmo, hallar los factores de $n = 158650368521$, sabiendo que $\varphi(n) = 158556411360$ y $\sigma(n) = 158744360544$.

4. Usar el Lema de Hensel para hallar las 6 soluciones de la ecuación $x^2 + x + 7 \equiv 0 \pmod{189}$ que vimos en clase.

5. Resolver las congruencias

   a) $x^5 + x^4 + 1 \equiv 0 \pmod{34}$,
   b) $x^3 + x + 57 \equiv 0 \pmod{53}$,
   c) $x^2 + 5x + 24 \equiv 0 \pmod{36}$,
   d) $x^1 1 + x^8 + 5 \equiv 0 \pmod{7}$.

6. Haga una implementación en Python del método $\rho$ de Pollard para hallar factores no triviales. Use este método, en conjunto con el test de Fermat (simple o fuerte), para hallar la factoración en primos de los siguiente números:

   a) $8,131$,
   b) $16,019$,
   c) $199,934,971$.

7. Alice y Bobo se quieren acordar una clave secreta $k$ mediante un protocolo de intercambio de Diffie-Hellman. Alice anuncia que su clave pública es $p = 3793$ y $g = 7$. Bob elige secretamente una clave privada, y elige de forma aleatoria un número $1 < b < p$ y envía a Alice el resultado $g^b \equiv 454 \pmod{p}$. ¿Cuál es la clave secreta?