Teoría de Números 2022

Lista 05

29.septiembre.2022

1. Suponga que $b \equiv a^{67} \pmod{91}$ y que $(a, 91) = 1$. Hallar un entero positivo k tal que $b^k \equiv a \pmod{91}$. Si $b \equiv 53 \pmod{91}$, ¿cuánto vale $a \pmod{91}$?

2. Sea $m = pq$ producto de dos primos distintos, y sea $\varphi = \varphi(m) = (p-1)(q-1)$ el valor de la función totiente de Euler en m. Hallar una fórmula para p y para q en términos de m y φ.

   Asumiendo que $m =$ 39,247,771 es producto de dos primos distintos, usar esta fórmula para encontrar p y q, sabiendo que $\varphi(m) =$39,233,944.

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

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 ρ 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) $199,934,971$.