MAT-120 Tarea 11

Teoría de Números

Fecha limite: 27 de noviembre de 2023

1. Sea p un primo impar. Demostrar que:

a) Las únicas soluciones de $x^2 \equiv 1 \pmod{p}$ son $x \equiv 1, -1 \pmod{p}$.

b) Las soluciones de $x^{p-2} + \cdots + x + 1 \equiv 0 \pmod{p}$ son $x \equiv 2, 3, \ldots, p-1 \pmod{p}$.

[Consejo: Factorizar $x^p - x$, y utilizar el TPF.]

2. Demostrar que, si p es un primo impar y $(a, p) = 1$, entonces $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$.

3. Sea r una raíz primitiva de un primo impar p. Demostrar:

a) r no es un residuo cuadrática de p.

b) Si r' es otra raíz primitiva de p, entonces rr' no es una raíz primitiva de p.

4. Hallar las soluciones de la ecuación $x^d - 1 \equiv 0 \pmod{13}$ para cada divisor d de $\phi(13)$.

b) Hacer el mismo, reemplazando 13 con 12.

5. Sea r una raíz primitiva del primo impar p. Demostrar:

a) Si $p \equiv 1 \pmod{4}$, entonces $-r$ también es una raíz primitiva de p.

b) Si $p \equiv 3 \pmod{4}$, entonces $\mathrm{ord}_p(-r) = \frac{p-1}{2}$.

6. Sea a un residuo cuadrática del primo impar p. Demostrar que $p - a$ es un residuo de p si $p \equiv 1 \pmod{4}$ y un residuo no cuadrático de p si $p \equiv 3 \pmod{4}$.

7. Evaluar los siguientes símbolos de Legendre. Utilizar el Teorema 9.2 y el Criterio de Euler (cuando apriopiado) para hacer la vida más fácil.

a) $(19/23)$

b) $(2/73)$

c) $(20/31)$

d) $(11/43)$

e) $(6/31)$

8. Sea p un primo impar. Demostrar que $(-1/p) = \begin{cases} 1 & \text{si } p \equiv 1 \pmod{4} \\ -1 & \text{si } p \equiv 3 \pmod{4} \end{cases}$

[Consejo: Teorema 9.2.]