Instituto Tecnológico de Estudios Superiores de Monterrey, Campus Guadalajara

MA2006B.401

Actividad 3 - Símbolo de Legendre y Residuos Cuadráticos

Uso de álgebras modernas para seguridad y criptografía

Equipo:
Alberto Cortés
Diego Pérez
Luis Ramírez
Mariana Rizo

3 de Abril del 2022

Problema 1

Usar el Teorema 1.1 para transformar cada uno de los siguientes polinomios cuadráticos en la forma $x^2 \equiv a\ (mod\ p)$:

a) $f(x) = 2 - x + 3x^2$ en $\mathbb{F}_7(x)$.

$$\begin{aligned} 3x^2 - x + 2 &\equiv 0\ (mod\ 7) \\ 36x^2 - 12x + 24 &\equiv 0\ (mod\ 7) \\ (6x-1)^2 + 23 &\equiv 0\ (mod\ 7) \\ (6x-1)^2 &\equiv -23\ (mod\ 7) \\ (6x-1)^2 &\equiv 5\ (mod\ 7) \end{aligned}$$

Como 5 no es un residuo cuadrático módulo 7, la congruencia no tiene solución.

b) $f(x) = 1 + 2x - x^2$ en $\mathbb{F}_{13}(x)$.

$$1 + 2x - x^2 \equiv 0(mod\ 13)$$
$$4x^2 - 8x - 4 \equiv 0(mod\ 13)$$
$$(2x-2)^2 - 8 \equiv 0(mod\ 13)$$
$$(2x-2)^2 \equiv 8(mod\ 13)$$

$$y = 2x - x$$
$$y^2 \equiv 8(mod\ 13)$$

Como 8 no es un residuo cuadrático módulo 13, la congruencia no tiene solución.

c) $f(x) = -2 - 7x + 14x^2$ en $\mathbb{F}_{17}(x)$.

$$14x^2 - 7x - 2 \equiv 0\ (mod\ 17)$$
$$784x^2 - 392x - 112 \equiv 0\ (mod\ 17)$$
$$(28x-7)^2 - 161 \equiv 0\ (mod\ 17)$$
$$(28x-7)^2 \equiv 161\ (mod\ 17)$$
$$(28x-7)^2 \equiv 8\ (mod\ 17)$$

$$y = 28x - 7$$
$$y^2 \equiv 8\ (mod\ 17)$$
$$y \equiv 5\ (mod\ 17)$$
$$28x - 7 \equiv 5\ (mod\ 17)$$
$$28x \equiv 12\ (mod\ 17)$$
$$x_1 \equiv 15\ (mod\ 17)$$

$$y \equiv 15\ (mod\ 17)$$
$$28x - 7 \equiv 15\ (mod\ 17)$$
$$28x \equiv 5\ (mod\ 17)$$
$$11x \equiv 5\ (mod\ 17)$$
$$x_2 \equiv 2\ (mod\ 17)$$

Problema 2

Demostrar la parte 2 del Teorema 2.2.

2. $a \equiv b \ (mod\ p) \implies \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

$$\begin{aligned} \left(\frac{a}{p}\right) &\equiv a^{\frac{p-1}{2}} \ (mod\ p) \\ = \left(\frac{b}{p}\right) &\equiv b^{\frac{p-1}{2}} \ (mod\ p) \\ a^{\frac{p-1}{2}} \ (mod\ p) &\equiv b^{\frac{p-1}{2}} \ (mod\ p) \\ \left(\frac{a}{p}\right) &= \left(\frac{b}{p}\right) \end{aligned}$$