Álgebra II. Hoja de ejercicios 12: Ecuaciones sobre cuerpos finitos
Universidad de El Salvador, ciclo par 2018

Por cualquier pregunta, no duden en escribir al grupo ues-algebra-2@googlegroups.com.

Ejercicio 1. *Para un entero de Gauss no invertible* $\alpha = a + b\sqrt{-1} \in \mathbb{Z}[\sqrt{-1}]$ *demuestre que*

$$\alpha \equiv 1 \pmod{2 + 2\sqrt{-1}}$$

si y solo si se cumple una de las dos condiciones:

1) $a \equiv 1$ *y* $b \equiv 0 \pmod 4$;

2) $a \equiv 3$ *y* $b \equiv 2 \pmod 4$.

Ejercicio 2. *Usando los resultados que vimos en clase, encuentre la cardinalidad del conjunto*

$$E_0(\mathbb{F}_p) := \{(x, y) \in \mathbb{A}^2(\mathbb{F}_p) \mid y^2 = x^3 - x\}$$

para $p = 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97$.

Ejercicio 3. *Demuestre que si* $p \equiv 1 \pmod 4$, *entonces el número* $\#E(\mathbb{F}_p) = \#E_0(\mathbb{F}_p) + 1$ *es siempre divisible por* 4.

Ejercicio 4. *Consideremos*

$$Z(t) = \frac{1 + 3\,t + 5t^2}{(1 - t)\,(1 - 5\,t)} \in \mathbb{Q}(t).$$

1) *Exprese* $Z(t)$ *como una serie*

$$1 + \underbrace{a_1\,t + a_2\,t^2 + a_3\,t^3 + a_4\,t^4 + \cdots}_{=:f} \in \mathbb{Q}[\![t]\!]$$

(calcule por lo menos los coeficientes a_1 *y* a_2*).*

2) *Calcule los coeficientes* b_1 *y* b_2 *de la serie*

$$\log(1 + f) := \sum_{k \geq 1} (-1)^{k+1}\,\frac{f^k}{k} = b_1\,t + \frac{b_2}{2}\,t^2 + \frac{b_3}{3}\,t^3 + \frac{b_4}{4}\,t^4 + \cdots \in \mathbb{Q}[\![t]\!]$$

Ejercicio 5. *Consideremos el espacio afín de dimensión n sobre el cuerpo finito* $\mathbb{F}_{q^k}$*:*

$$\mathbb{A}^n(\mathbb{F}_{q^k}) = \mathbb{F}_{q^k}^n.$$

Encuentre la expresión racional para la función zeta

$$Z(\mathbb{A}^n_{/\mathbb{F}_q}, t) := \exp\left(\sum_{k \geq 1} \#\mathbb{A}^n(\mathbb{F}_{q^k})\,\frac{t^k}{k}\right).$$

Ejercicio 6. *Para los conjuntos*

$$V(\mathbb{F}_{q^k}) := \{(x, y) \in \mathbb{A}^2(\mathbb{F}_{q^k}) \mid xy = 0\},$$
$$W(\mathbb{F}_{q^k}) := \{(x, y) \in \mathbb{A}^2(\mathbb{F}_{q^k}) \mid x^2 - y^2 = 0\}$$

encuentre la expresión racional para $Z(V_{/\mathbb{F}_q}, t)$ *y* $Z(W_{/\mathbb{F}_q}, t)$.