Facultad de Ciencias Exactas, Ingeniería y Agrimensura
Escuela de Ciencias Exactas y Naturales
Departamento de Matemática

Licenciatura en Ciencias de la Computación

Álgebra y Geometría Analítica II (2015)

Cuerpos finitos

1. *a*) Probar que $\sqrt{2}$ es irracional.

   b) Probar que si $a, b \in \mathbb{Q}$, no ambos nulos, entonces $a^2 - 2b^2 \neq 0$.

2. *a*) Considerar la ecuación $x^2 + 1 = 0$. Decidir si tiene solución para $x \in \mathbb{R}, \mathbb{C}, \mathbb{Z}_2, \mathbb{Z}_3$.

   b) Ídem con la ecuación $x^2 + x + 1 = 0$.

3. Escribir las tablas de sumar y multiplicar para $\mathbb{Z}_4$, $\mathbb{Z}_6$ y $\mathbb{Z}_8$. Explicar porque $\mathbb{Z}_4$, $\mathbb{Z}_6$ y $\mathbb{Z}_8$ no son cuerpos.

4. Escribir las tablas de sumar y multiplicar para $\mathbb{F} = \mathbb{Z}_7$, $\mathbb{Z}_{11}$ y $\mathbb{Z}_{13}$. Encontrar 2^{-1}, 5^{-1} y 6^{-1} en cada uno de estos cuerpos. ¿Qué elementos de $\mathbb{F}$ les corresponden a las expresiones 26, 5/8 y 33/12?

5. Sean p un número primo y $1 \leq k \leq p - 1$.

   a) Probar que el número combinatorio $\binom{p}{k}$ es múltiplo de p. ¿Sigue siendo cierta la afirmación si no se asume p primo? *Ayuda*: se tiene que

   $$\binom{p}{k} = \frac{p!}{(p-k)!k!} = \frac{p(p-1)\cdots(p-k+1)}{k(k-1)\cdots 2 \cdot 1}$$

   es un número natural, se debería mostrar que ninguno de los números $2, 3, \ldots, k-1, k$ se simplifica con p, de donde sigue que

   $$\frac{(p-1)\cdots(p-k+1)}{k(k-1)\cdots 2 \cdot 1}$$

   es un número natural.

   b) Concluir que para todos $a, b \in \mathbb{Z}_p$ vale

   $$(a+b)^p = a^p + b^p.$$

6. Resolver los siguientes sistemas de ecuaciones lineales

   a) $\begin{cases} x + 2y + w = 0 \\ x + y + z = 0 \\ 2x + y + 2z + 2w = 0 \end{cases}$ sobre $\mathbb{Z}_3$

   b) $\begin{cases} x + 2y + 4z = 2 \\ x + 3y + z = 4 \end{cases}$ sobre $\mathbb{Z}_5$

$c)$ $\begin{cases} x+y=0 \\ y+z+w=1 \\ x+z+w=1 \end{cases}$ sobre $\mathbb{Z}_2$

7. Decidir si las matrices $\begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 4 & 1 & 3 \\ 1 & 2 & 0 \\ 0 & 3 & 2 \end{pmatrix}$ y $\begin{pmatrix} 2 & 6 & 1 \\ 1 & 4 & 2 \\ 0 & 3 & 1 \end{pmatrix}$ tienen inversa sobre $\mathbb{Z}_2$, $\mathbb{Z}_5$ y $\mathbb{Z}_7$ respectivamente. Encontrar la inversa en caso afirmativo.

8. Se sabe que el sistema de ecuaciones lineales sobre $\mathbb{Q}$

$$\begin{cases} 1000000x + 1000001y = 415267172223 \\ 10000000y + 9999999z = 2845679887655 \\ 999998x + 999999y + 1000000z = 527611341689 \end{cases}$$

tiene solución única $x, y, z \in \mathbb{Z}$. Determinar la paridad de la solución (sin resolver el sistema).

9. Usando ecuaciones lineales con coeficientes en $\mathbb{Z}_7$ determinar:

   $a)$ qué día de la semana será su cumpleaños número 50;

   $b)$ qué día de la semana será navidad en el año 3000;

   $c)$ qué día de la semana falleció el Gral. San Martín (1778–1850).

10. Sea $\mathbb{F}$ un cuerpo arbitrario. La matriz de Vandermonde asociada a los elementos $a_1, \dots, a_n \in \mathbb{F}$ se define como

$$V = \begin{pmatrix} 1 & a_1 & a_1^2 & \cdots & a_1^{n-1} \\ 1 & a_2 & a_2^2 & \cdots & a_2^{n-1} \\ 1 & a_3 & a_3^2 & \cdots & a_3^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_n & a_n^2 & \cdots & a_n^{n-1} \end{pmatrix}.$$

Probar que

$$\det V = \prod_{i<j} (a_j - a_i).$$

En particular, V es invertible si $a_1, \dots, a_n$ son distintos dos a dos. *Ayuda*: hará falta usar operaciones elementales por columnas, el desarrollo del determinante por la primera fila e inducción.

11. Encontrar un polinomio $Q(x)$ con coeficientes en $\mathbb{Z}_p$ tal que $Q(x) = 2^x$ para $p = 5$ y $p = 7$.