# Introducción a la Teoría de Códigos

M.A. García, L. Martínez, T. Ramírez

Facultad de Ciencia y Tecnología. UPV/EHU

## Resumen Teórico
## Apartado A3 del Anexo:
## Ejemplos de cuerpos finitos

Mayo de 2017

# A.3. Ejemplos de cuerpos finitos

En esta sección veremos algunos ejemplos de cuerpos finitos de orden pequeño. Para construir un cuerpo de orden $p^n$ es necesario conocer un polinomio irreducible de grado $n$ con coeficientes en $\mathbb{Z}/p\mathbb{Z}$. Por lo general, no hay un único polinomio irreducible de grado $n$ en $\mathbb{Z}/p\mathbb{Z}[x]$ aunque, por lo visto en la Proposición A.2.6, todos ellos dan lugar a cuerpos isomorfos.

Dentro de los polinomios irreducibles $P(x)$, interesan especialmente aquellos que cumplen que las potencias $\overline{x}^i$ permiten obtener todos los elementos no nulos del cuerpo $\mathbb{Z}/p\mathbb{Z}[x]/(P(x))$. Dichos polinomios se llaman **primitivos**. El conocer estos polinomios es importante en algunas áreas de la Teoría de Códigos, como por ejemplo cuando se estudian los códigos BCH.

Por ejemplo, el polinomio $x^2+1 \in \mathbb{Z}/3\mathbb{Z}[x]$ es irreducible, pero no es primitivo, ya que al hacer las potencias de $\overline{x}$ obtenemos:

$\overline{x}^0 = \overline{1}$,

$\overline{x}^1 = \overline{x}$,

$\overline{x}^2 = \overline{2}$,

$\overline{x}^3 = \overline{2x}$,

$\overline{x}^5 = \overline{1}$,

y de ahí en adelante se van repitiendo cíclicamente los mismos cuatro elementos. Por lo tanto, al hacer potencias de $\overline{x}$ sólo se obtienen $\overline{1}, \overline{x}, \overline{2}, \overline{2x}$, y no se consiguen todos los 8 elementos no nulos del cuerpo.

En cambio, el polinomio $x^2+2x+2 \in \mathbb{Z}/3\mathbb{Z}$, además de irreducible es primitivo, ya que las potencias de $\overline{x}$ dan:

$\overline{x}^0 = \overline{1}$,

$\overline{x}^1 = \overline{x}$,

$\overline{x}^2 = \overline{x+1}$,

$\overline{x}^3 = \overline{2x+1}$,

$\overline{x}^4 = \overline{2}$,

$\overline{x}^5 = \overline{2x}$,

$\overline{x}^6 = \overline{2x+2}$,

$\overline{x}^7 = \overline{x+2}$,

y en este caso sí obtenemos los 8 elementos distintos de cero del cuerpo. Al seguir haciendo potencias, estos 8 elementos se van repitiendo cíclicamente.

**Proposición A.3.1** *Si $p$ es un número primo y $n$ es un número natural, hay por lo menos un polinomio primitivo de grado $n$ en $\mathbb{Z}/p\mathbb{Z}[x]$.*

Por lo general, no hay un sólo polinomio primitivo de grado $n$ en $\mathbb{Z}/p\mathbb{Z}[x]$. Por ejemplo, en $\mathbb{Z}/2\mathbb{Z}[x]$ hay dos polinomios primitivos de grado 3: $1+x+x^3$ y $1+x^2+x^3$.

En la tabla siguiente damos un ejemplo de un polinomio primitivo de grados 2,3,4,5 para los primos 2,3,5,7,11,13.

| | $n=2$ | $n=3$ | $n=4$ | $n=5$ |
|---|---|---|---|---|
| $p=2$ | $x^2+x+1$ | $x^3+x^2+1$ | $x^4+x+1$ | $x^5+x^4+x^3+x^2+1$ |
| $p=3$ | $x^2+2x+2$ | $x^3+2x^2+x+1$ | $x^4+x^3+2x^2+2x+2$ | $x^5+x^4+2x^3+x^2+x+1$ |
| $p=5$ | $x^2+3x+3$ | $x^3+4x+3$ | $x^4+4x^2+x+2$ | $x^5+2x^4+3x^3+x^2+4x+2$ |
| $p=7$ | $x^2+x+3$ | $x^3+3x^2+4$ | $x^4+3x^2+4x+3$ | $x^5+x^4+5x^3+2x^2+4$ |
| $p=11$ | $x^2+4x+7$ | $x^3+2x^2+6x+9$ | $x^4+4x^2+x+2$ | $x^5+x^4+9x^3+3x^2+5x+5$ |
| $p=13$ | $x^2+4x+11$ | $x^3+7x^2+2x+6$ | $x^4+4x^2+x+2$ | $x^5+x^4+x^3+11x^2+8x+6$ |

Para terminar, veamos un ejemplo de cómo podemos utilizar los datos de la tabla para calcular el inverso en un cuerpo finito. Consideramos un cuerpo de orden 8, utilizando el polinomio primitivo $x^3+x^2+1$ de dicha tabla, es decir, tomemos

$$\mathbb{Z}/2\mathbb{Z}[x]/(x^3+x^2+1).$$

Vamos a calcular el inverso de $\overline{x^2+1}$. Como $x^2+1$ y $x^3+x^2+1$ son primos entre sí en $\mathbb{Z}/2\mathbb{Z}[x]$, utilizando el algoritmo de Euclides extendido obtenemos

$$1=(x^2+x+1)(x^2+1)-x(x^3+x^2+1),$$

luego el inverso de $\overline{x^2+1}$ es $\overline{x^2+x+1}$.