Tema 4

Polinomios

4.1 Anillo de polinomios con coeficientes en un cuerpo

Aunque se puede definir el conjunto de los polinomios con coeficientes en un anillo, nuestro estudio se va a centrar en el conjunto de los polinomios con coeficientes en un cuerpo.

Definición 4.1 (Anillo de polinomios) *El anillo de polinomios con coeficientes en un cuerpo K, es el conjunto*

$$K[X] = \{ a_0 + a_1X + \ldots + a_nX^n, a_i \in K \}$$

junto con las operaciones suma y producto definidos en la forma usual.
Dados $f(X) = \sum_{i=}^{r} a_iX^i$ y $g(X) = \sum_{i=0}^{s} b_iX^i \in K[X]$, se definen:

Suma: $f(X) + g(X) = \sum_{i=0}^{n}(a_i + b_i)X^i$, siendo $n = \max\{r, s\}$

Producto: $f(X).g(X) = \sum_{i=0}^{r+s}\left(\sum_{j=0}^{i} a_j\, b_{i-j}\right)X^i$

$K[X]$ con las dos operaciones definidas tiene estructura de anillo conmutativo con identidad.

Todo polinomio no nulo puede escribirse en la forma $f(X) = \sum_{i=}^{d} a_iX^i$ con $a_d \neq 0$ para algún $d \geq 0$. En este caso, el número natural d se dice grado del polinomio y lo denotaremos por $gr(f)$. Al coeficiente a_d se le dice *coeficiente director*.
De lo anterior se deduce que las constantes (los elementos de K) son polinomios de grado cero. Asimismo, se define $gr(0) = -\infty$.
El grado verifica:

I) $gr(f + g)) \leq \max\{ gr(f), gr(g)\}$
II) $gr(f . g)) = gr(f) + gr(g)$

En lo referente a divisibilidad, el anillo de polinomios tiene un comportamiento análogo al anillo de los números enteros. Es un dominio de integridad y posee división euclídea, el papel del valor absoluto lo juega ahora el grado.

Proposición 4.2 *El anillo* $(K[X], +, .)$ *es un dominio de integridad. Esto significa que el producto de dos polinomios no puede ser 0 si ambos son no nulos.*

Demostración.
Dados $f(x) = \sum_{i=0}^{r} a_iX^i$, $g(x) = \sum_{i=0}^{s} b_iX^i \in K[x]$, $f(x) \neq 0$ y verificando $f(x).g(x) = 0$, veamos que $g(x) = 0$.
Al ser $f(x) \neq 0$, tiene algún coeficiente no nulo. Se puede suponer, sin pérdida de generalidad, que $a_0 \neq 0$. Si fuese a_k el primer coeficiente no nulo, esto es $a_k \neq 0$ y $a_i = 0$

$\forall\ i$ con $0 \le i \le k$-1, se tendría $f(x) = \sum_{i=k}^{r} a_i X^i = X^k\left(\sum_{i=k}^{r} a_i X^{i-k}\right)$, y se podría trabajar con el polinomio$\sum_{i=k}^{r} a_i X^{i-k}$.
Supongamos que $a_0 \neq 0$
Si $f(x).g(x) = \sum_{i=0}^{r+s}\left(\sum_{j=0}^{i} a_j\, b_{i-j}\right)X^i = 0$, todos los coeficientes son nulos, esto es, $\sum_{j=0}^{i} a_j\, b_{i-j} = 0$, para $i \in \{0, \ldots, r+s\}$. Veamos por inducción que $b_i = 0$.
Para $i = 0$, se tiene $0 = a_0 b_0$. De $a_0 \neq 0$ se deduce $b_0 = 0$.
Supongamos cierto que $b_j = 0$ para $1 \le j \le k-1$, veamos que $b_k = 0$:
$0 = \sum_{j=0}^{k} a_j\, b_{k-j} = a_0 b_k$, De $a_0 \neq 0$ se deduce $b_k = 0$. Por tanto $g(x) = 0$ ■

Todo lo que sabemos de $\mathbb{Z}$ con respecto al máximo común divisor, algoritmo de Euclides, identidad de Bézout, factorización única de primos, ecuaciones diofánticas lineales, … funciona exactamente igual en el caso de los anillos de polinomios $K[X]$.

Definición 4.3 (División euclídea)
En el caso de los enteros se tenía una aplicación (el valor absoluto):

$$|\,.\,| : \mathbb{Z} \to \mathbb{N}$$

Y que dados cualesquiera a y b, $b \neq 0$, existirían q y r tales que:

$$a = b\,.\,q + r, \text{ con } 0 \le r < |\,b\,|,$$

en el caso del anillo de polinomios el papel de esa aplicación lo juega la aplicación grado:

$$gr(.)\ K[X] \to \mathbb{N}$$

se tiene que, *para cualesquiera polinomios* $f(X)$ y $g(X)$, $g(X) \neq 0$, *existen polinomios* $q(X)$ y $r(X)$, *tales que*

$$f(X) = g(X)q(X) + r(X),\ gr(r) < gr(g)$$

A $q(X)$ se le denomina cociente y $r(X)$ resto.

Ejemplo 4.4 *Hallar el cociente y el resto de dividir* $x^5 + x^4 + 2x^3 + x^2 + 4x + 2$ entre $x^2+2x + 3$ en $\mathbb{Z}_7[x]$.

$(x^5 + x^4 + 2x^3 + x^2 + 4x + 2) = (x^2 + 2x + 3)(\, x^3 - x^2 + x + 2) + (-3x - 4) \equiv$
$(x^2 + 2x + 3)(\, x^3 + 6x^2 + x + 2) + (4x + 3)(\text{mód } 7)$
Cociente $x^3 + 6x^2 + x + 2$, Resto $4x + 3$ ■

Proposición 4.5 *Los únicos elementos inversibles en el anillo* $K[X]$ *son las constantes.*

Demostración.
Es consecuencia de las propiedades del grado.
Sea $f(X) \in K[X]$ un elemento inversible, existe $g(X) \in K[X]$ verificando $f(X)g(X) = 1$.
En consecuencia, $f(X)$ y $g(X)$ son polinomios no nulos y $gr(f.g)\ ) = gr(f) + gr(g) = 0$. Por tanto $gr(f) = gr(g) = 0$, es decir, son constantes. ■

Definición 4.6 *Un polinomio* $g(X)$ *se dice* ***divisor*** *(o* ***factor****) de* $f(X)$ *en* $K[X]$ *si existe un polinomio* $h(X)$ *en* $K[X]$ *tal que* $f(X) = g(X)\ h(X)$.

Definición 4.7 (**Polinomios mónicos)** *Se llaman polinomios mónicos a aquellos cuyo coeficiente director es* 1.

Estos polinomios mónicos juegan el papel, que en el caso de los enteros juegan los números positivos. Del mismo modo que en $\mathbb{Z}$, todo entero se podía escribir como el producto de una unidad (±1) por un entero positivo, en este caso todo polinomio puede escribirse como una unidad en $K[X]$ por un polinomio Mónico. En efecto, $f(X) = \sum_{i=}^{d} a_i X^i$, al ser $a_d \neq 0$, se puede poner en la forma:

$$f(X) = a_d \left(X^d + \frac{a_{d-1}}{a_d} X^{d-1} + \frac{a_{d-2}}{a_d} X^{d-2} + \cdots + \frac{a_1}{a_d} X + \frac{a_0}{a_d} \right)$$

Definición 4.8 (**Polinomios irreducibles)** *Un polinomio mónico no constante se dice irreducible* (*o primo*) *si los únicos polinomios mónicos que lo dividen son el 1 y el propio polinomio.*

Usando el mismo argumento que en el caso de los enteros, se puede demostrar que existen infinitos.
Los polinomios mónicos de grado 1 son todos irreducibles, independientemente del cuerpo de coeficientes *K*..
En general, la forma de los polinomios irreducibles depende del cuerpo de coeficientes. Así, se tiene:

- K = $\mathbb{Q}$. Existen polinomio irreducibles de cualquier grado. Por ejemplo, $X^n + p$ es irreducible para cualquier entero primo p (si no fuese primo tampoco lo sería p).
- K = $\mathbb{R}$. Los polinomios primos son de dos tipos:
  - $X - \alpha$, para cualquier $X - \alpha$, número real.
  - $(X - \alpha)^2 + \beta^2$. Los $\alpha \in \mathbb{R}$ y $\beta \in \mathbb{R}\setminus\{0\}$.
- K = $\mathbb{C}$. Los únicos polinomios irreducibles son los mónicos de grado uno. (Teorema fundamental del Álgebra).
- K = $\mathbb{Z}_p$. Existen polinomios irreducibles de cualquier grado.

Definición 4.9 (Máximo común divisor) *Dados dos polinomios el máximo común divisor es el único polinomio mónico que verifica:*

i) Divide a ambos.
ii) Todo divisor de ambos es también divisor de él.

Algoritmo 4.10 (Algoritmo de Euclides) En un anillo de polinomios existe un proceso similar al que conocemos en los enteros para el cálculo del máximo común divisor de dos polinomios. En este caso el polinomio resto tiene grado estrictamente menor que el divisor. El proceso termina cuando el resto es 0. También se cumple la identidad de Bézout.

Ejemplo 4.11 *Encontrar el máximo común divisor y una identidad de Bézout de los polinomios* $g(X) = X^3 + 1$ y $f(X) = X^4 + X^3 + 2X^2 + X + 1$ de $\mathbb{Q}[X]$.

Vamos a realizar el proceso matricial similar al que conocemos para los enteros, hay que ir anotando los cocientes en cada paso que se da en el algoritmo.

$$R_0 = \begin{pmatrix} X^4 + X^3 + 2X^2 + X + 1 & X^3 + 1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Dado que $f(X) = X^4 + X^3 + 2X^2 + X + 1 = (X^3 + 1)(X + 1) + 2X^2$

$$Q_1 = \begin{pmatrix} 0 & 1 \\ 1 & -(X+1) \end{pmatrix}$$

$$R_1 = R_0Q_1 = \begin{pmatrix} X^3 + 1 & 2X^2 \\ 0 & 1 \\ 1 & -(X+1) \end{pmatrix}$$

Al ser $X^3 + 1 = (2\,X^2).\frac{1}{2}X + 1$

$$Q_2 = \begin{pmatrix} 0 & 1 \\ 1 & -\frac{1}{2}X \end{pmatrix}$$

$$R_2 = R_0Q_1Q_2 = \begin{pmatrix} 2X^2 & 1 \\ 1 & -\frac{1}{2}X \\ -(X-1) & \frac{1}{2}X^2 + \frac{1}{2}X + 1 \end{pmatrix}$$

Al ser $2\,X^2 = 1.2X^2$

$$Q_3 = \begin{pmatrix} 0 & 1 \\ 1 & -2X^2 \end{pmatrix}$$

$$R_3 = R_0Q_1Q_2Q_3 = \begin{pmatrix} 1 & 0 \\ -\frac{1}{2}X & \mathrm{X}^3 \\ \frac{1}{2}X^2 + \frac{1}{2}X + 1 & -X^4 - X^3 - 2X^2 - x + 1 \end{pmatrix}$$

El proceso ha terminado, el máximo común divisor es 1. Los polinomios son coprimos. Se deduce la siguiente identidad de Bézout

$$1 = \left(-\tfrac{1}{2}X\right) f(X) + \left(\tfrac{1}{2}X^2 + \tfrac{1}{2}X + 1\right) g(X) \qquad \blacksquare$$

4.2 Factorización de polinomios

Los polinomios irreducibles juegan el mismo papel en los anillos de polinomios que jugaban los números primos en los enteros.

4.2.1 Factorización de polinomios con coeficientes en un cuerpo.

Teorema 4.12 *Todo polinomio no constante K*[*x*] *se puede expresar como producto de polinomios irreducibles. La factorización es única salvo producto por constantes y reordenaciones de los factores.*

Teorema 4.13 *Sea K un cuerpo y f*(*X*) *un polinomio de K*[*x*]. *Se verifica:*
X-α *es divisor de f*(*X*) *si, y sólo si, f*(α) = 0 *en K.*

Demostración.
Supongamos que *X-*α es divisor de *f*(*X*). Existe $g(X) \in K[x]$ tal que $f(X) = (X-\alpha)g(X)$.
Al evaluar α en *f*(*X*) se tiene $f(\alpha) = (\alpha-\alpha)g(X) = 0$ $g(X) = 0$.
Recíprocamente, supongamos que $f(\alpha) = 0$.
Al hacer la división euclídea de *f*(*X*) por (*X-*α), existen *q*(*X*) y *r*(*X*) tal que
$f(X) = (X-\alpha)q(X) + r(X)$, con $gr(r(X)) < gr(X-\alpha)$ ó $r(X) = 0$.

En consecuencia, $r(X)$ es una constante.
Por otra parte, al sustituir X por α, se tiene $0 = f(\alpha) = (\alpha-\alpha)q(X) + r(\alpha) = r(\alpha)$.
Por tanto $r(X) = 0$. ■

Teorema 4.14 *Sea K un cuerpo, y* $f(X) \in K[x]$ *con grado* $n \geq 1$, *se verifica que la ecuación* $f(X) = 0$ *tiene a lo más n raíces ven K.*

Demostración. Supongamos que tiene m raíces distintas $\alpha_1, \alpha_2, \ldots, \alpha_m$ en K. Por el teorema anterior $f(X) = (X-\alpha_1)(X-\alpha_2)\ldots(X-\alpha_m)g(X)$ para algún $g(X) \in K[x]$.
Se verifica que el grado de $f(X)$ es la suma de los grados de los factores. Con lo cual, $gr(f(X)) = m + gr(f(X)) \geq m$
De lo que se deduce que el grado de $f(X)$ es al menos m, esto es, $n \geq m$.

Por otra parte, en un cuerpo $\mathbb{Z}_p$ (p primo) hallar las raíces de un polinomio es un proceso finito, basta evaluar el polinomio en los p elementos del cuerpo.

4.2.2 Factorización de polinomios con coeficientes en un cuerpo $\mathbb{Z}_p$.

Teorema 4.15. *En* $\mathbb{Z}_p[x]$ *existen polinomios irreducibles de todos los grados.*

Demostración. Veamos la demostración para grados 1 y 2.
Los polinomios lineales son irreducibles en $\mathbb{Z}_p[x]$. Por tanto hay p polinomios irreducibles $X + \alpha$, para cada $\alpha \in \mathbb{Z}_p$.

Si un polinomio cuadrático $X^2 + a_1X + a_0$ es reducible en $\mathbb{Z}_p[x]$, es producto de dos factores lineales. Como hay p factores lineales posibles, habrá $\frac{p(p-1)}{2}$ polinomios cuadráticos mónicos reducibles $(X-\alpha)(X-\beta)$ con $\alpha \neq \beta$ y p de la forma $(X-\alpha)^2$.
Por otra parte, hay p^2 polinomios cuadráticos mónicos en total.
Por tanto hay $p^2 - \frac{p(p-1)}{2} - p = \frac{p(p-1)}{2}$ polinomios irreducibles cuadráticos. ■

Se puede demostrar que existen polinomios irreducibles de cualquier grado.

Ejemplo 4.16 *Factorizar en* $\mathbb{Z}_3[x]$ *el polinomio* $x^4 + 1$.

Hallamos primero las raíces:
$f(x) = x^4 + 1$.

$f(0) = 0^4 + 1 = 1$, $f(1) = 1^4 + 1 = 2$, $f(2) = 2^4 + 1 = 5 \equiv 2 \ (mod\ 3)$

No tiene raíces, por tanto no hay factores lineales en la factorización. Sólo se podrá factorizar con dos polinomios cuadráticos.
$f(x) = x^4 + 1 = (x^2 + Ax + B)(x^2 + Cx + D)$, con A, B, C y D en $\mathbb{Z}_4$.
$f(x) = x^4 + 1 = (x^2 + Ax + B)(x^2 + Cx + D) = x^4+(A+C)x^3+(AC+B+D)\ x^2+(AD+BC)x+BD$

Igualando coeficientes de las potencias de x se tiene:
$A+C \equiv 0\ (mod\ 3)$, $AC+B+D \equiv 0\ (mod\ 3)$, $AD+BC \equiv 0\ (mod\ 3)$, $BD \equiv 1\ (mod\ 3)$
Resolviendo el sistema se obtiene $A = 1$, $B = C = D = 2$

Por tanto $x^4 + 1 = (x^2 + x + 2)(x^2 + 2x + 2)$. ■

4.2.3 Raíces de polinomios con coeficientes en un anillo $\mathbb{Z}_m$.

En este vamos a ver cómo se pueden encontrar raíces de polinomios cuando los coeficientes están en un anillo $\mathbb{Z}_m$.
Para ello hay que recordar que todo número entero se puede poner como producto de potencias de primos.

Observación 4.17 Para encontrar las soluciones módulo una potencia de primo se reduce el proceso a la potencia anterior. Si se quiere resolver $f(x) \equiv 0 \pmod{p^k}$ con p primo y k entero positivo con $k \geq 2$. Puesto que, todo múltiplo de p^k lo es también de p^{k-1}, se pueden encontrar las soluciones de $f(x) \equiv 0 \pmod{p^{k-1}}$ y, de entre ellas, las que verifican la ecuación dada.

Ejemplo 4.18 *Calcular las soluciones de* $2x^3 + 2x - 4 \equiv 0$ (*mod* 5)
$\mathbb{Z}_5$ es un cuerpo.

Son las soluciones en $\mathbb{Z}_5$ a lo más hay 5. Por comprobación calculamos cuales son: Sólo al sustituir x por 1 se obtiene un resultado múltiplo de 5.
La única solución es $x = \overline{1}$. ■

Ejemplo 4.19 *Calcular las soluciones de* $2x^3 + 7x - 4 \equiv 0$ (*mod* 25)
$\mathbb{Z}_{25}$ es un anillo, no es un cuerpo.
Puesto que todo múltiplo de 25 lo es de 5, las soluciones lo tendrán que ser también de $2x^3 + 7x - 4 \equiv 0 \pmod 5$. Busquemos las soluciones de esa ecuación
$2x^3 + 7x - 4 \equiv 2x^3 + 2x - 4 \equiv 0 \pmod 5$. Hemos visto anteriormente que la única solución en $\mathbb{Z}_5$ es $x = \overline{1}$, esto es $x = 1 + 5t$.
Volviendo a $\mathbb{Z}_{25}$ hay que buscar soluciones de que lo sean a la vez de

$$2x^3 + 7x - 4 \equiv 0 \pmod{25} \text{ y } x \equiv 1 \pmod 5$$

Al ser $x = 1 + 5t$ sustituimos en la ecuación de partida:

$$2(1 + 5t)^3 + 7(1 + 5t) - 4 \equiv 0 \pmod{25}$$

Operando $65t + 5 \equiv 15t + 5 \equiv 0 \pmod{25}$, $15t \equiv -5 \pmod{25} \equiv 20 \pmod{25}$, resolviendo la congruencia $t = 8 + 5s \equiv 8 \pmod 5 \equiv 3 \pmod 5$, $t = 3 + 5k$
$x = 1 + 5t = 1 + 5(3 + 5k) = 16 + 25k \equiv 16 \pmod{25}$
En $\mathbb{Z}_{25}$ la única solución es $\overline{16}$. ■

Ejemplo 4.20 *Calcular las soluciones de* $2x^3 + 7x - 4 \equiv 0$ (*mod* 8)
$8 = 2^3$,

- En primer lugar buscamos las que verifican $2x^3 + 7x - 4 \equiv 0 \pmod 2$

$2x^3 + 7x - 4 \equiv x \equiv 0 \pmod 2$, la solución es de la forma $x = 2t$

- Después buscamos las que verifican $2x^3 + 7x - 4 \equiv 0 \pmod 4$.
- $2x^3 + 7x - 4 \equiv 2x^3 + 3x \equiv 0 \pmod 4$. Sabemos que son de la forma $x = 2t$. Sustituimos: $2(2t)^3 + 3(2t) \equiv 6t \equiv 2t \equiv 0 \pmod 4$.

Resolviendo la congruencia $t = 2s$, $x = 2t = 4s$.

- Por último, hay que resolver $2x^3 + 7x - 4 \equiv 0 \pmod 8$. De entre las soluciones obtenidas anteriormente hay que ver cuales la verifican

$2x^3 + 7x - 4 \equiv 2(4s)^3 + 7(4s) - 4 \equiv 4s - 4 \equiv 0 \pmod 8$, $4s \equiv 4 \pmod 8$, $s = 3 + 2k$

$x = 4s = 4(3 + 2k) = 12 + 8k \equiv 4 (mod\ 8)$ ■

Ejemplo 4.21 *Calcular las soluciones de* $2x^3 + 7x - 4 \equiv 0\ (mod\ 200)$
La factorización en primos de 200 es $2^3 5^2 = 8 * 25$
Resolver la ecuación dada es equivalente a resolver el sistema

$$2x^3 + 7x - 4 \equiv 0\ (mod\ 25) \text{ y } 2x^3 + 7x - 4 \equiv 0\ (mod\ 8)$$

Cada una de las ecuaciones están resueltas en ejemplos anteriores:
Las soluciones de $2x^3 + 7x - 4 \equiv 0\ (mod\ 8)$ son $x \equiv 4 (mod\ 8)$
Las soluciones de $2x^3 + 7x - 4 \equiv 0\ (mod\ 25)$ son $x \equiv 16 (mod\ 25)$
Usando el teorema chino de los restos resuelve el sistema $x \equiv 4 (mod\ 8)$, $x \equiv 16 (mod\ 25)$.
Se obtiene $x \equiv 116 (mod\ 200)$, estas son las soluciones de la ecuación dada. ■

4.3 Cuerpos finitos

En este apartado vamos a indicar como se pueden construir cuerpos finitos de cardinal potencia de primos.

Al igual que en el caso de los enteros, se puede definir la relación de equivalencia ser congruente módulo un polinomio mónico $f(X) \in K[X]$:

Definición 4.22 (Congruencias)
Dos polinomios $g(X)$ *y* $h(X)$ *en* $K[X]$ *se dicen congruentes módulo un polinomio mónico* $f(X)$ *si, y sólo si,* $f(X)$ *divide a* $g(X) - h(X)$:

$$g(X) \equiv h(X)\ (mod\ f(X)) \Leftrightarrow g(X) - h(X) \text{ es múltiplo de } f(X).$$

Del mismo modo que en el caso de los enteros, se puede dotar al conjunto cociente resultante de la relación de equivalencia anterior estructura de anillo. Habitualmente, este anillo se denota por:

$$K[X] / f(X)$$

Teorema 4.23 *El anillo* $K[X] / f(X)$ *es un cuerpo si, y sólo si,* $f(X)$ *es un polinomio irreducible.*

La identidad de Bézout garantiza la existencia de inverso de cada polinomio no nulo.
Los polinomios de grados menores estrictamente que el grado de $f(X)$ constituyen un conjunto completo de representantes de las clases de equivalencia. Si dicho grado es α, al haber p^α polinomios distintos de grado menor estrictamente que α, el número de clases de equivalencia es igual a p^α.

Teorema 4.24 *Sea K un cuerpo finito, se verifica que* $|K| = p^\alpha$, *con p primo.*

Este teorema indica que el cardinal de los cuerpos finitos es igual a una potencia de un número primo. Por otra parte, el teorema 4.15 nos dice que, dada cualquier potencia de primo, existe un cuerpo con ese cardinal.

Ejemplo 4.20 *Construir un cuerpo con exactamente 9 elementos.*
Puesto que $9 = 3^2$, si $p(x)$ es un polinomio irreducible en $\mathbb{Z}_3[x]$ de grado 2, $\mathbb{Z}_3[x]/(p(x))$ tiene estructura de cuerpo y 9 elementos. Hay que buscar un polinomio irreducible de grado 2.

Para construir un cuerpo con 9 elementos, únicamente hay que encontrar un polinomio irreducible de grado 2 en $\mathbb{Z}_3[x]$.
x^2+1 es un polinomio irreducible de grado 2 en $\mathbb{Z}_3[x]$, basta comprobar que 0, 1, y 2 no son soluciones.
Vamos a construir el conjunto cociente $\mathbb{Z}_3[x]/(x^2+1)$, es un cuerpo con 9 elementos

Sean $g(X), h(X) \in \mathbb{Z}_3[x]$ la relación es:

$$g(X) \equiv h(X) \ (mod\ x^2+1) \Leftrightarrow g(X) - h(X) \text{ es múltiplo de } x^2+1$$

Vamos a ver qué clases hay. Recordar que en $\mathbb{Z}_3$ se verifica $x^2 \equiv 1$ (*mod* 3).

$0, 1, 2, x, x+1, x+2, 2x, 2x+1, 2x+2$ forman un sistema completo de representantes de las clases de equivalencia.
El conjunto $\{\bar{0}, \bar{1}, \bar{2}, \bar{x}, \overline{x+1}, \overline{x+2}, \overline{2x}, \overline{2x+1}, \overline{2x+2}\}$ de las clases de equivalencia de la congruencia módulo x^2+1 en $\mathbb{Z}_3[x]$, con la suma y el producto de polinomios tiene estructura de cuerpo. Es un cuerpo de 9 elementos.
Observación:
La clase de $\bar{1}$ representa a todos los polinomios de $\mathbb{Z}_3[x]$ de la forma 1+ múltiplo de (x^2+1)
El inverso de $\overline{2x+1}$ es $\overline{2x+2}$, basta observar que
$(2x+1)(2x+2) = 4x^2+6x+2 = x^2+2$ en $\mathbb{Z}_3$ y $(2x+1)(2x+2) = 1 + (x^2+1) \equiv 1$ mód(x^2+1)

Las siguientes tablas muestran la suma y el producto en este cuerpo:

+	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
0	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
1	1	2	0	$x+1$	$x+2$	x	$2x+1$	$2x+2$	$2x$
2	2	0	1	$x+2$	x	$x+1$	$2x+2$	$2x$	$2x+1$
x	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$	0	1	2
$x+1$	$x+1$	$x+2$	x	$2x+1$	$2x+2$	$2x$	1	2	0
$x+2$	$x+2$	x	$x+1$	$2x+2$	$2x$	$2x+1$	2	0	1
$2x$	$2x$	$2x+1$	$2x+2$	0	1	2	x	$x+1$	$x+2$
$2x+1$	$2x+1$	$2x+2$	$2x$	1	2	0	$x+1$	$x+2$	x
$2x+2$	$2x+2$	$2x$	$2x+1$	2	0	1	$x+2$	x	$x+1$

*	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
2	0	2	1	$2x$	$2x+2$	$2x+1$	x	$x+2$	$x+1$
x	0	x	$2x$	2	$x+2$	$2x+2$	1	$x+1$	$2x+1$
$x+1$	0	$x+1$	$2x+2$	$x+2$	$2x$	1	$2x+1$	2	x
$x+2$	0	$x+2$	$2x+1$	$2x+2$	1	x	$x+1$	$2x$	2
$2x$	0	$2x$	x	1	$2x+1$	$x+1$	2	$2x+2$	$x+2$
$2x+1$	0	$2x+1$	$x+2$	$x+1$	2	$2x$	$2x+2$	x	1
$2x+2$	0	$2x+2$	$x+1$	$2x+1$	x	2	$x+2$	1	$2x$

Inverso de 1 es 1

Son inversos x y $2x$

Son inversos $x+1$ y $x+2$

Son inversos $2x+1$ y $2x+2$