Inversos modulares de polinomios.

Inversos modulares de polinomios.

Antes de realizar algunos ejemplos de cálculo, hemos de tener en cuenta lo siguiente:

Inversos modulares de polinomios.

Antes de realizar algunos ejemplos de cálculo, hemos de tener en cuenta lo siguiente:

- *El maximo común divisor de dos polinomios no nulos es* **siempre** *un polinomio mónico.*

Inversos modulares de polinomios.

Antes de realizar algunos ejemplos de cálculo, hemos de tener en cuenta lo siguiente:

- *El maximo común divisor de dos polinomios no nulos es* **siempre** *un polinomio mónico.*
- *Al calcular el máximo común divisor por el algoritmo de Euclides, puede ocurrir que el último resto no nulo no sea un polinomio mónico.*

Inversos modulares de polinomios.

Antes de realizar algunos ejemplos de cálculo, hemos de tener en cuenta lo siguiente:

- *El maximo común divisor de dos polinomios no nulos es* **siempre** *un polinomio mónico.*
- *Al calcular el máximo común divisor por el algoritmo de Euclides, puede ocurrir que el último resto no nulo no sea un polinomio mónico.*
- *En tal caso, el resultado final deberá multiplicarse por el inverso del coeficiente líder.*

Inversos modulares de polinomios.

Antes de realizar algunos ejemplos de cálculo, hemos de tener en cuenta lo siguiente:

- *El maximo común divisor de dos polinomios no nulos es* **siempre** *un polinomio mónico.*
- *Al calcular el máximo común divisor por el algoritmo de Euclides, puede ocurrir que el último resto no nulo no sea un polinomio mónico.*
- *En tal caso, el resultado final deberá multiplicarse por el inverso del coeficiente líder.*
- *Si aplicamos el algoritmo extendido de Euclides, esta operación habremos de repetirla para los polinomios $u(x)$ y $v(x)$.*

Inversos modulares de polinomios.

Antes de realizar algunos ejemplos de cálculo, hemos de tener en cuenta lo siguiente:

- *El maximo común divisor de dos polinomios no nulos es* **siempre** *un polinomio mónico.*
- *Al calcular el máximo común divisor por el algoritmo de Euclides, puede ocurrir que el último resto no nulo no sea un polinomio mónico.*
- *En tal caso, el resultado final deberá multiplicarse por el inverso del coeficiente líder.*
- *Si aplicamos el algoritmo extendido de Euclides, esta operación habremos de repetirla para los polinomios* $u(x)$ *y* $v(x)$.
- *Puesto que el cálculo de inversos modulares se realiza con el algoritmo extendido de Euclides, cuando calculemos inversos modulares de polinomios deberemos tener esto presente.*

Inversos modulares de polinomios.

Antes de realizar algunos ejemplos de cálculo, hemos de tener en cuenta lo siguiente:

- *El maximo común divisor de dos polinomios no nulos es* **siempre** *un polinomio mónico.*
- *Al calcular el máximo común divisor por el algoritmo de Euclides, puede ocurrir que el último resto no nulo no sea un polinomio mónico.*
- *En tal caso, el resultado final deberá multiplicarse por el inverso del coeficiente líder.*
- *Si aplicamos el algoritmo extendido de Euclides, esta operación habremos de repetirla para los polinomios $u(x)$ y $v(x)$.*
- *Puesto que el cálculo de inversos modulares se realiza con el algoritmo extendido de Euclides, cuando calculemos inversos modulares de polinomios deberemos tener esto presente.*

A continuación realizaremos el cálculo de algunos inversos.

Inversos de polinomios modulares. Ejemplo 1

Inversos de polinomios modulares. Ejemplo 1

Sea $A = \mathbb{Z}_7[x]_{x^4+2x^3+x+4}$ y $q(x) = x^3 + 3x^2 + 5x + 2$.

Inversos de polinomios modulares. Ejemplo 1

Sea $A = \mathbb{Z}_7[x]_{x^4+2x^3+x+4}$ y $q(x) = x^3 + 3x^2 + 5x + 2$.
Vamos a calcular, si es posible, $q(x)^{-1}$ (en A).

Inversos de polinomios modulares. Ejemplo 1

Sea $A = \mathbb{Z}_7[x]_{x^4+2x^3+x+4}$ y $q(x) = x^3 + 3x^2 + 5x + 2$.
Vamos a calcular, si es posible, $q(x)^{-1}$ (en A).
En primer lugar comprobamos si dicho inverso existe.

Inversos de polinomios modulares. Ejemplo 1

Sea $A = \mathbb{Z}_7[x]_{x^4+2x^3+x+4}$ y $q(x) = x^3 + 3x^2 + 5x + 2$.
Vamos a calcular, si es posible, $q(x)^{-1}$ (en A).
En primer lugar comprobamos si dicho inverso existe.
Para ello, hemos de ver si $\mathrm{mcd}(x^4 + 2x^3 + x + 4, x^3 + 3x^2 + 5x + 2)$ vale o no vale 1.

Inversos de polinomios modulares. Ejemplo 1

Sea $A = \mathbb{Z}_7[x]_{x^4+2x^3+x+4}$ y $q(x) = x^3 + 3x^2 + 5x + 2$.
Vamos a calcular, si es posible, $q(x)^{-1}$ (en A).
En primer lugar comprobamos si dicho inverso existe.
Para ello, hemos de ver si $\mathrm{mcd}(x^4 + 2x^3 + x + 4, x^3 + 3x^2 + 5x + 2)$ vale o no vale 1.
Realizamos las correspondientes divisiones:

Inversos de polinomios modulares. Ejemplo 1

Sea $A = \mathbb{Z}_7[x]_{x^4+2x^3+x+4}$ y $q(x) = x^3 + 3x^2 + 5x + 2$.
Vamos a calcular, si es posible, $q(x)^{-1}$ (en A).
En primer lugar comprobamos si dicho inverso existe.
Para ello, hemos de ver si $\mathrm{mcd}(x^4 + 2x^3 + x + 4, x^3 + 3x^2 + 5x + 2)$ vale o no vale 1.
Realizamos las correspondientes divisiones:

$$x^4 + 2x^3 + x + 4 \quad = \quad (x^3 + 3x^2 + 5x + 2) \cdot c_1(x) + r_1(x)$$

Inversos de polinomios modulares. Ejemplo 1

Sea $A = \mathbb{Z}_7[x]_{x^4+2x^3+x+4}$ y $q(x) = x^3 + 3x^2 + 5x + 2$.
Vamos a calcular, si es posible, $q(x)^{-1}$ (en A).
En primer lugar comprobamos si dicho inverso existe.
Para ello, hemos de ver si $\mathrm{mcd}(x^4 + 2x^3 + x + 4, x^3 + 3x^2 + 5x + 2)$ vale o no vale 1.
Realizamos las correspondientes divisiones:

$$x^4 + 2x^3 + x + 4 = (x^3 + 3x^2 + 5x + 2) \cdot (x + 6) + (5x^2 + 4x + 6)$$

Inversos de polinomios modulares. Ejemplo 1

Sea $A = \mathbb{Z}_7[x]_{x^4+2x^3+x+4}$ y $q(x) = x^3 + 3x^2 + 5x + 2$.
Vamos a calcular, si es posible, $q(x)^{-1}$ (en A).
En primer lugar comprobamos si dicho inverso existe.
Para ello, hemos de ver si $\mathrm{mcd}(x^4 + 2x^3 + x + 4, x^3 + 3x^2 + 5x + 2)$ vale o no vale 1.
Realizamos las correspondientes divisiones:

$$\begin{aligned}
x^4 + 2x^3 + x + 4 &= (x^3 + 3x^2 + 5x + 2) \cdot (x + 6) + 5x^2 + 4x + 6 \\
x^3 + 3x^2 + 5x + 2 &= (5x^2 + 4x + 6) \cdot c_2(x) + r_2(x)
\end{aligned}$$

Inversos de polinomios modulares. Ejemplo 1

Sea $A = \mathbb{Z}_7[x]_{x^4+2x^3+x+4}$ y $q(x) = x^3 + 3x^2 + 5x + 2$.
Vamos a calcular, si es posible, $q(x)^{-1}$ (en A).
En primer lugar comprobamos si dicho inverso existe.
Para ello, hemos de ver si $\text{mcd}(x^4 + 2x^3 + x + 4, x^3 + 3x^2 + 5x + 2)$ vale o no vale 1.
Realizamos las correspondientes divisiones:

$$\begin{aligned} x^4 + 2x^3 + x + 4 &= (x^3 + 3x^2 + 5x + 2) \cdot (x + 6) + 5x^2 + 4x + 6 \\ x^3 + 3x^2 + 5x + 2 &= (5x^2 + 4x + 6) \cdot (3x + 1) + (4x + 3) \end{aligned}$$

Inversos de polinomios modulares. Ejemplo 1

Sea $A = \mathbb{Z}_7[x]_{x^4+2x^3+x+4}$ y $q(x) = x^3 + 3x^2 + 5x + 2$.
Vamos a calcular, si es posible, $q(x)^{-1}$ (en A).
En primer lugar comprobamos si dicho inverso existe.
Para ello, hemos de ver si $\mathrm{mcd}(x^4 + 2x^3 + x + 4, x^3 + 3x^2 + 5x + 2)$ vale o no vale 1.
Realizamos las correspondientes divisiones:

$$\begin{aligned}
x^4 + 2x^3 + x + 4 &= (x^3 + 3x^2 + 5x + 2) \cdot (x + 6) + 5x^2 + 4x + 6 \\
x^3 + 3x^2 + 5x + 2 &= (5x^2 + 4x + 6) \cdot (3x + 1) + 4x + 3 \\
5x^2 + 4x + 6 &= (4x + 3) \cdot c_3(x) + r_3(x)
\end{aligned}$$

Inversos de polinomios modulares. Ejemplo 1

Sea $A = \mathbb{Z}_7[x]_{x^4+2x^3+x+4}$ y $q(x) = x^3 + 3x^2 + 5x + 2$.
Vamos a calcular, si es posible, $q(x)^{-1}$ (en A).
En primer lugar comprobamos si dicho inverso existe.
Para ello, hemos de ver si $\text{mcd}(x^4 + 2x^3 + x + 4, x^3 + 3x^2 + 5x + 2)$ vale o no vale 1.
Realizamos las correspondientes divisiones:

$$\begin{aligned}
x^4 + 2x^3 + x + 4 &= (x^3 + 3x^2 + 5x + 2) \cdot (x + 6) + 5x^2 + 4x + 6 \\
x^3 + 3x^2 + 5x + 2 &= (5x^2 + 4x + 6) \cdot (3x + 1) + 4x + 3 \\
5x^2 + 4x + 6 &= (4x + 3) \cdot (3x + 4) + (1)
\end{aligned}$$

Inversos de polinomios modulares. Ejemplo 1

Sea $A = \mathbb{Z}_7[x]_{x^4+2x^3+x+4}$ y $q(x) = x^3 + 3x^2 + 5x + 2$.
Vamos a calcular, si es posible, $q(x)^{-1}$ (en A).
En primer lugar comprobamos si dicho inverso existe.
Para ello, hemos de ver si $\mathrm{mcd}(x^4 + 2x^3 + x + 4, x^3 + 3x^2 + 5x + 2)$ vale o no vale 1.
Realizamos las correspondientes divisiones:

$$\begin{aligned} x^4 + 2x^3 + x + 4 &= (x^3 + 3x^2 + 5x + 2) \cdot (x + 6) + 5x^2 + 4x + 6 \\ x^3 + 3x^2 + 5x + 2 &= (5x^2 + 4x + 6) \cdot (3x + 1) + 4x + 3 \\ 5x^2 + 4x + 6 &= (4x + 3) \cdot (3x + 4) + (1) \end{aligned}$$

Inversos de polinomios modulares. Ejemplo 1

Sea $A = \mathbb{Z}_7[x]_{x^4+2x^3+x+4}$ y $q(x) = x^3 + 3x^2 + 5x + 2$.
Vamos a calcular, si es posible, $q(x)^{-1}$ (en A).
En primer lugar comprobamos si dicho inverso existe.
Para ello, hemos de ver si $\mathrm{mcd}(x^4 + 2x^3 + x + 4, x^3 + 3x^2 + 5x + 2)$ vale o no vale 1.
Realizamos las correspondientes divisiones:

$$\begin{aligned}
x^4 + 2x^3 + x + 4 &= (x^3 + 3x^2 + 5x + 2) \cdot (x + 6) + 5x^2 + 4x + 6 \\
x^3 + 3x^2 + 5x + 2 &= (5x^2 + 4x + 6) \cdot (3x + 1) + 4x + 3 \\
5x^2 + 4x + 6 &= (4x + 3) \cdot (3x + 4) + (1)
\end{aligned}$$

El resto de la última división es el polinomio constante 1 (que es mónico).

Inversos de polinomios modulares. Ejemplo 1

Sea $A = \mathbb{Z}_7[x]_{x^4+2x^3+x+4}$ y $q(x) = x^3 + 3x^2 + 5x + 2$.
Vamos a calcular, si es posible, $q(x)^{-1}$ (en A).
En primer lugar comprobamos si dicho inverso existe.
Para ello, hemos de ver si $\text{mcd}(x^4 + 2x^3 + x + 4, x^3 + 3x^2 + 5x + 2)$ vale o no vale 1.
Realizamos las correspondientes divisiones:

$$\begin{aligned}
x^4 + 2x^3 + x + 4 &= (x^3 + 3x^2 + 5x + 2) \cdot (x + 6) + 5x^2 + 4x + 6 \\
x^3 + 3x^2 + 5x + 2 &= (5x^2 + 4x + 6) \cdot (3x + 1) + 4x + 3 \\
5x^2 + 4x + 6 &= (4x + 3) \cdot (3x + 4) + (1)
\end{aligned}$$

El resto de la última división es el polinomio constante 1 (que es mónico).
Vemos entonces que $\text{mcd}(x^4 + 2x^3 + x + 4, x^3 + 3x^2 + 5x + 2) = 1$.

Inversos de polinomios modulares. Ejemplo 1

Sea $A = \mathbb{Z}_7[x]_{x^4+2x^3+x+4}$ y $q(x) = x^3 + 3x^2 + 5x + 2$.
Vamos a calcular, si es posible, $q(x)^{-1}$ (en A).
En primer lugar comprobamos si dicho inverso existe.
Para ello, hemos de ver si $\mathrm{mcd}(x^4 + 2x^3 + x + 4, x^3 + 3x^2 + 5x + 2)$ vale o no vale 1.
Realizamos las correspondientes divisiones:

$$\begin{array}{rcl} x^4 + 2x^3 + x + 4 & = & (x^3 + 3x^2 + 5x + 2) \cdot (x + 6) + 5x^2 + 4x + 6 \\ x^3 + 3x^2 + 5x + 2 & = & (5x^2 + 4x + 6) \cdot (3x + 1) + 4x + 3 \\ 5x^2 + 4x + 6 & = & (4x + 3) \cdot (3x + 4) + (1) \end{array}$$

El resto de la última división es el polinomio constante 1 (que es mónico).
Vemos entonces que $\mathrm{mcd}(x^4 + 2x^3 + x + 4, x^3 + 3x^2 + 5x + 2) = 1$.
Por tanto, existe el inverso de $q(x)$.

Inversos de polinomios modulares. Ejemplo 1

Sea $A = \mathbb{Z}_7[x]_{x^4+2x^3+x+4}$ y $q(x) = x^3 + 3x^2 + 5x + 2$.
Vamos a calcular, si es posible, $q(x)^{-1}$ (en A).
En primer lugar comprobamos si dicho inverso existe.
Para ello, hemos de ver si $\mathrm{mcd}(x^4 + 2x^3 + x + 4, x^3 + 3x^2 + 5x + 2)$ vale o no vale 1.
Realizamos las correspondientes divisiones:

$$\begin{aligned}
x^4 + 2x^3 + x + 4 &= (x^3 + 3x^2 + 5x + 2) \cdot (x + 6) + 5x^2 + 4x + 6 \\
x^3 + 3x^2 + 5x + 2 &= (5x^2 + 4x + 6) \cdot (3x + 1) + 4x + 3 \\
5x^2 + 4x + 6 &= (4x + 3) \cdot (3x + 4) + (1)
\end{aligned}$$

El resto de la última división es el polinomio constante 1 (que es mónico).
Vemos entonces que $\mathrm{mcd}(x^4 + 2x^3 + x + 4, x^3 + 3x^2 + 5x + 2) = 1$.
Por tanto, existe el inverso de $q(x)$.
Los resultados obtenidos los distribuimos en la siguiente tabla:

Inversos de polinomios modulares. Ejemplo 1

Sea $A = \mathbb{Z}_7[x]_{x^4+2x^3+x+4}$ y $q(x) = x^3 + 3x^2 + 5x + 2$.
Vamos a calcular, si es posible, $q(x)^{-1}$ (en A).
En primer lugar comprobamos si dicho inverso existe.
Ya hemos visto que dicho inverso existe.

$x^4 + 2x^3 + x + 4$		0
$x^3 + 3x^2 + 5x + 2$		1
$5x^2 + 4x + 6$	$x + 6$	$v_1(x)$
$4x + 3$	$3x + 1$	$v_2(x)$
1	$3x + 4$	$v_3(x)$

Inversos de polinomios modulares. Ejemplo 1

Sea $A = \mathbb{Z}_7[x]_{x^4+2x^3+x+4}$ y $q(x) = x^3 + 3x^2 + 5x + 2$.
Vamos a calcular, si es posible, $q(x)^{-1}$ (en A).
En primer lugar comprobamos si dicho inverso existe.
Ya hemos visto que dicho inverso existe.

$x^4 + 2x^3 + x + 4$		0
$x^3 + 3x^2 + 5x + 2$		1
$5x^2 + 4x + 6$	$x + 6$	$v_1(x)$
$4x + 3$	$3x + 1$	$v_2(x)$
1	$3x + 4$	$v_3(x)$

$v_1(x) = 0 - (x + 6) \cdot 1$

Inversos de polinomios modulares. Ejemplo 1

Sea $A = \mathbb{Z}_7[x]_{x^4+2x^3+x+4}$ y $q(x) = x^3 + 3x^2 + 5x + 2$.
Vamos a calcular, si es posible, $q(x)^{-1}$ (en A).
En primer lugar comprobamos si dicho inverso existe.
Ya hemos visto que dicho inverso existe.

$x^4 + 2x^3 + x + 4$		0
$x^3 + 3x^2 + 5x + 2$		1
$5x^2 + 4x + 6$	$x + 6$	$v_1(x)$
$4x + 3$	$3x + 1$	$v_2(x)$
1	$3x + 4$	$v_3(x)$

$v_1(x) = 0 - (x + 6) \cdot 1 = 6x + 1.$

Sea $A=\mathbb{Z}_7[x]_{x^4+2x^3+x+4}$ y $q(x)=x^3+3x^2+5x+2$.
Vamos a calcular, si es posible, $q(x)^{-1}$ (en A).
En primer lugar comprobamos si dicho inverso existe.
Ya hemos visto que dicho inverso existe.

x^4+2x^3+x+4		0
x^3+3x^2+5x+2		1
$5x^2+4x+6$	$x+6$	$6x+1$
$4x+3$	$3x+1$	$v_2(x)$
1	$3x+4$	$v_3(x)$

Inversos de polinomios modulares. Ejemplo 1

Sea $A = \mathbb{Z}_7[x]_{x^4+2x^3+x+4}$ y $q(x) = x^3 + 3x^2 + 5x + 2$.
Vamos a calcular, si es posible, $q(x)^{-1}$ (en A).
En primer lugar comprobamos si dicho inverso existe.
Ya hemos visto que dicho inverso existe.

$x^4 + 2x^3 + x + 4$		0
$x^3 + 3x^2 + 5x + 2$		1
$5x^2 + 4x + 6$	$x + 6$	$6x + 1$
$4x + 3$	$3x + 1$	$v_2(x)$
1	$3x + 4$	$v_3(x)$

$v_2(x) = 1 - (3x + 1) \cdot (6x + 1)$

Sea $A = \mathbb{Z}_7[x]_{x^4+2x^3+x+4}$ y $q(x) = x^3 + 3x^2 + 5x + 2$.
Vamos a calcular, si es posible, $q(x)^{-1}$ (en A).
En primer lugar comprobamos si dicho inverso existe.
Ya hemos visto que dicho inverso existe.

$x^4 + 2x^3 + x + 4$		0
$x^3 + 3x^2 + 5x + 2$		1
$5x^2 + 4x + 6$	$x + 6$	$6x + 1$
$4x + 3$	$3x + 1$	$v_2(x)$
1	$3x + 4$	$v_3(x)$

$v_1(x) = 1 - (3x + 1) \cdot (6x + 1) = 1 + (4x + 6) \cdot (6x + 1)$

Inversos de polinomios modulares. Ejemplo 1

Sea $A = \mathbb{Z}_7[x]_{x^4+2x^3+x+4}$ y $q(x) = x^3 + 3x^2 + 5x + 2$.
Vamos a calcular, si es posible, $q(x)^{-1}$ (en A).
En primer lugar comprobamos si dicho inverso existe.
Ya hemos visto que dicho inverso existe.

$x^4 + 2x^3 + x + 4$		0
$x^3 + 3x^2 + 5x + 2$		1
$5x^2 + 4x + 6$	$x + 6$	$6x + 1$
$4x + 3$	$3x + 1$	$v_2(x)$
1	$3x + 4$	$v_3(x)$

$v_1(x) = 1 - (3x + 1) \cdot (6x + 1) = 1 + (4x + 6) \cdot (6x + 1) = 3x^2 + 5x.$

Inversos de polinomios modulares. Ejemplo 1

Sea $A = \mathbb{Z}_7[x]_{x^4+2x^3+x+4}$ y $q(x) = x^3 + 3x^2 + 5x + 2$.
Vamos a calcular, si es posible, $q(x)^{-1}$ (en A).
En primer lugar comprobamos si dicho inverso existe.
Ya hemos visto que dicho inverso existe.

$x^4 + 2x^3 + x + 4$		0
$x^3 + 3x^2 + 5x + 2$		1
$5x^2 + 4x + 6$	$x + 6$	$6x + 1$
$4x + 3$	$3x + 1$	$3x^2 + 5x$
1	$3x + 4$	$v_3(x)$

Sea $A = \mathbb{Z}_7[x]_{x^4+2x^3+x+4}$ y $q(x) = x^3 + 3x^2 + 5x + 2$.
Vamos a calcular, si es posible, $q(x)^{-1}$ (en A).
En primer lugar comprobamos si dicho inverso existe.
Ya hemos visto que dicho inverso existe.

x^4+2x^3+x+4		0
x^3+3x^2+5x+2		1
$5x^2+4x+6$	$x+6$	$6x+1$
$4x+3$	$3x+1$	$3x^2+5x$
1	$3x+4$	$v_3(x)$

$v_3(x) = 6x + 1 - (3x+4)\cdot(3x^2+5x)$

Inversos de polinomios modulares. Ejemplo 1

Sea $A = \mathbb{Z}_7[x]_{x^4+2x^3+x+4}$ y $q(x) = x^3 + 3x^2 + 5x + 2$.
Vamos a calcular, si es posible, $q(x)^{-1}$ (en A).
En primer lugar comprobamos si dicho inverso existe.
Ya hemos visto que dicho inverso existe.

$x^4 + 2x^3 + x + 4$		0
$x^3 + 3x^2 + 5x + 2$		1
$5x^2 + 4x + 6$	$x + 6$	$6x + 1$
$4x + 3$	$3x + 1$	$3x^2 + 5x$
1	$3x + 4$	$v_3(x)$

$$v_3(x) = 6x + 1 - (3x + 4) \cdot (3x^2 + 5x) = 6x + 1 + (4x + 3) \cdot (3x^2 + 5x)$$

Inversos de polinomios modulares. Ejemplo 1

Sea $A = \mathbb{Z}_7[x]_{x^4+2x^3+x+4}$ y $q(x) = x^3 + 3x^2 + 5x + 2$.
Vamos a calcular, si es posible, $q(x)^{-1}$ (en A).
En primer lugar comprobamos si dicho inverso existe.
Ya hemos visto que dicho inverso existe.

$x^4 + 2x^3 + x + 4$		0
$x^3 + 3x^2 + 5x + 2$		1
$5x^2 + 4x + 6$	$x + 6$	$6x + 1$
$4x + 3$	$3x + 1$	$3x^2 + 5x$
1	$3x + 4$	$v_3(x)$

$$v_3(x) = 6x + 1 - (3x + 4) \cdot (3x^2 + 5x) = 6x + 1 + (4x + 3) \cdot (3x^2 + 5x) = 5x^3 + x^2 + 1.$$

Inversos de polinomios modulares. Ejemplo 1

Sea $A = \mathbb{Z}_7[x]_{x^4+2x^3+x+4}$ y $q(x) = x^3 + 3x^2 + 5x + 2$.
Vamos a calcular, si es posible, $q(x)^{-1}$ (en A).
En primer lugar comprobamos si dicho inverso existe.
Ya hemos visto que dicho inverso existe.

$x^4 + 2x^3 + x + 4$		0
$x^3 + 3x^2 + 5x + 2$		1
$5x^2 + 4x + 6$	$x + 6$	$6x + 1$
$4x + 3$	$3x + 1$	$3x^2 + 5x$
1	$3x + 4$	$5x^3 + x^2 + 1$

Sea $A = \mathbb{Z}_7[x]_{x^4+2x^3+x+4}$ y $q(x) = x^3 + 3x^2 + 5x + 2$.
Vamos a calcular, si es posible, $q(x)^{-1}$ (en A).
En primer lugar comprobamos si dicho inverso existe.
Ya hemos visto que dicho inverso existe.

$x^4 + 2x^3 + x + 4$		0
$x^3 + 3x^2 + 5x + 2$		1
$5x^2 + 4x + 6$	$x + 6$	$6x + 1$
$4x + 3$	$3x + 1$	$3x^2 + 5x$
1	$3x + 4$	$5x^3 + x^2 + 1$

Y ya tenemos calculado el inverso.

Inversos de polinomios modulares. Ejemplo 1

Sea $A = \mathbb{Z}_7[x]_{x^4+2x^3+x+4}$ y $q(x) = x^3 + 3x^2 + 5x + 2$.
Vamos a calcular, si es posible, $q(x)^{-1}$ (en A).
En primer lugar comprobamos si dicho inverso existe.
Ya hemos visto que dicho inverso existe.

$x^4 + 2x^3 + x + 4$		0
$x^3 + 3x^2 + 5x + 2$		1
$5x^2 + 4x + 6$	$x + 6$	$6x + 1$
$4x + 3$	$3x + 1$	$3x^2 + 5x$
1	$3x + 4$	$5x^3 + x^2 + 1$

Y ya tenemos calculado el inverso.
Dicho inverso vale:

Inversos de polinomios modulares. Ejemplo 1

Sea $A = \mathbb{Z}_7[x]_{x^4+2x^3+x+4}$ y $q(x) = x^3 + 3x^2 + 5x + 2$.
Vamos a calcular, si es posible, $q(x)^{-1}$ (en A).
En primer lugar comprobamos si dicho inverso existe.
Ya hemos visto que dicho inverso existe.

$x^4 + 2x^3 + x + 4$		0
$x^3 + 3x^2 + 5x + 2$		1
$5x^2 + 4x + 6$	$x + 6$	$6x + 1$
$4x + 3$	$3x + 1$	$3x^2 + 5x$
1	$3x + 4$	$5x^3 + x^2 + 1$

Y ya tenemos calculado el inverso.
Dicho inverso vale:

$$5x^3 + x^2 + 1$$

Inversos de polinomios modulares. Ejemplo 1

Sea $A = \mathbb{Z}_7[x]_{x^4+2x^3+x+4}$ y $q(x) = x^3 + 3x^2 + 5x + 2$.
Vamos a calcular, si es posible, $q(x)^{-1}$ (en A).
Ya hemos visto que $q(x)^{-1} = 5x^3 + x^2 + 1$.

Inversos de polinomios modulares. Ejemplo 1

Sea $A = \mathbb{Z}_7[x]_{x^4+2x^3+x+4}$ y $q(x) = x^3 + 3x^2 + 5x + 2$.
Vamos a calcular, si es posible, $q(x)^{-1}$ (en A).
Ya hemos visto que $q(x)^{-1} = 5x^3 + x^2 + 1$.
Vamos a comprobarlo.

Inversos de polinomios modulares. Ejemplo 1

Sea $A = \mathbb{Z}_7[x]_{x^4+2x^3+x+4}$ y $q(x) = x^3 + 3x^2 + 5x + 2$.
Vamos a calcular, si es posible, $q(x)^{-1}$ (en A).
Ya hemos visto que $q(x)^{-1} = 5x^3 + x^2 + 1$.
Vamos a comprobarlo.
Para eso, multiplicamos $q(x)$ por $5x^3 + x^2 + 1$.

Inversos de polinomios modulares. Ejemplo 1

Sea $A = \mathbb{Z}_7[x]_{x^4+2x^3+x+4}$ y $q(x) = x^3 + 3x^2 + 5x + 2$.
Vamos a calcular, si es posible, $q(x)^{-1}$ (en A).
Ya hemos visto que $q(x)^{-1} = 5x^3 + x^2 + 1$.
Vamos a comprobarlo.
Para eso, multiplicamos $q(x)$ por $5x^3 + x^2 + 1$.

$$\begin{array}{cccc} 1 & 3 & 5 & 2 \\ 5 & 1 & 0 & 1 \\ \hline \end{array}$$

Inversos de polinomios modulares. Ejemplo 1

Sea $A = \mathbb{Z}_7[x]_{x^4+2x^3+x+4}$ y $q(x) = x^3 + 3x^2 + 5x + 2$.
Vamos a calcular, si es posible, $q(x)^{-1}$ (en A).
Ya hemos visto que $q(x)^{-1} = 5x^3 + x^2 + 1$.
Vamos a comprobarlo.
Para eso, multiplicamos $q(x)$ por $5x^3 + x^2 + 1$.

$$\begin{array}{rrrr} 1 & 3 & 5 & 2 \\ 5 & 1 & 0 & 1 \\ \hline 1 & 3 & 5 & 2 \end{array}$$

Inversos de polinomios modulares. Ejemplo 1

Sea $A = \mathbb{Z}_7[x]_{x^4+2x^3+x+4}$ y $q(x) = x^3 + 3x^2 + 5x + 2$.
Vamos a calcular, si es posible, $q(x)^{-1}$ (en A).
Ya hemos visto que $q(x)^{-1} = 5x^3 + x^2 + 1$.
Vamos a comprobarlo.
Para eso, multiplicamos $q(x)$ por $5x^3 + x^2 + 1$.

$$
\begin{array}{ccccccc}
 & & & 1 & 3 & 5 & 2 \\
 & & & 5 & 1 & 0 & 1 \\
\hline
 & & & 1 & 3 & 5 & 2 \\
1 & 3 & 5 & 2 & & &
\end{array}
$$

Inversos de polinomios modulares. Ejemplo 1

Sea $A = \mathbb{Z}_7[x]_{x^4+2x^3+x+4}$ y $q(x) = x^3 + 3x^2 + 5x + 2$.
Vamos a calcular, si es posible, $q(x)^{-1}$ (en A).
Ya hemos visto que $q(x)^{-1} = 5x^3 + x^2 + 1$.
Vamos a comprobarlo.
Para eso, multiplicamos $q(x)$ por $5x^3 + x^2 + 1$.

$$\begin{array}{ccccccc}
 & & & 1 & 3 & 5 & 2 \\
 & & & 5 & 1 & 0 & 1 \\
\cline{3-7}
 & & & 1 & 3 & 5 & 2 \\
 & 1 & 3 & 5 & 2 & & \\
5 & 1 & 4 & 3 & & &
\end{array}$$

Inversos de polinomios modulares. Ejemplo 1

Sea $A = \mathbb{Z}_7[x]_{x^4+2x^3+x+4}$ y $q(x) = x^3 + 3x^2 + 5x + 2$.
Vamos a calcular, si es posible, $q(x)^{-1}$ (en A).
Ya hemos visto que $q(x)^{-1} = 5x^3 + x^2 + 1$.
Vamos a comprobarlo.
Para eso, multiplicamos $q(x)$ por $5x^3 + x^2 + 1$.

$$\begin{array}{ccccccc}
 & & & 1 & 3 & 5 & 2 \\
 & & & 5 & 1 & 0 & 1 \\
\cline{3-7}
 & & & 1 & 3 & 5 & 2 \\
 & 1 & 3 & 5 & 2 & & \\
5 & 1 & 4 & 3 & & & \\
\hline
5 & 2 & 0 & 2 & 5 & 5 & 2
\end{array}$$

Inversos de polinomios modulares. Ejemplo 1

Sea $A = \mathbb{Z}_7[x]_{x^4+2x^3+x+4}$ y $q(x) = x^3 + 3x^2 + 5x + 2$.
Vamos a calcular, si es posible, $q(x)^{-1}$ (en A).
Ya hemos visto que $q(x)^{-1} = 5x^3 + x^2 + 1$.
Vamos a comprobarlo.
$(x^3 + 3x^2 + 5x + 2) \cdot (5x^3 + x^2 + 1) = 5x^6 + 2x^5 + 2x^3 + 5x^2 + 5x + 2$

$$
\begin{array}{ccccccc}
 & & & 1 & 3 & 5 & 2 \\
 & & & 5 & 1 & 0 & 1 \\
\hline
 & & & 1 & 3 & 5 & 2 \\
 & 1 & 3 & 5 & 2 & & \\
5 & 1 & 4 & 3 & & & \\
\hline
5 & 2 & 0 & 2 & 5 & 5 & 2
\end{array}
$$

Inversos de polinomios modulares. Ejemplo 1

Sea $A = \mathbb{Z}_7[x]_{x^4+2x^3+x+4}$ y $q(x) = x^3 + 3x^2 + 5x + 2$.
Vamos a calcular, si es posible, $q(x)^{-1}$ (en A).
Ya hemos visto que $q(x)^{-1} = 5x^3 + x^2 + 1$.
Vamos a comprobarlo.
$(x^3 + 3x^2 + 5x + 2) \cdot (5x^3 + x^2 + 1) = 5x^6 + 2x^5 + 2x^3 + 5x^2 + 5x + 2$
Dividimos este polinomio entre $x^4 + 2x^3 + x + 4$.

Inversos de polinomios modulares. Ejemplo 1

Sea $A = \mathbb{Z}_7[x]_{x^4+2x^3+x+4}$ y $q(x) = x^3 + 3x^2 + 5x + 2$.
Vamos a calcular, si es posible, $q(x)^{-1}$ (en A).
Ya hemos visto que $q(x)^{-1} = 5x^3 + x^2 + 1$.
Vamos a comprobarlo.
$(x^3 + 3x^2 + 5x + 2) \cdot (5x^3 + x^2 + 1) = 5x^6 + 2x^5 + 2x^3 + 5x^2 + 5x + 2$
Dividimos este polinomio entre $x^4 + 2x^3 + x + 4$.
El resto debe ser 1.

Inversos de polinomios modulares. Ejemplo 1

Sea $A = \mathbb{Z}_7[x]_{x^4+2x^3+x+4}$ y $q(x) = x^3 + 3x^2 + 5x + 2$.
Vamos a calcular, si es posible, $q(x)^{-1}$ (en A).
Ya hemos visto que $q(x)^{-1} = 5x^3 + x^2 + 1$.
Vamos a comprobarlo.
$(x^3 + 3x^2 + 5x + 2) \cdot (5x^3 + x^2 + 1) = 5x^6 + 2x^5 + 2x^3 + 5x^2 + 5x + 2$
Dividimos este polinomio entre $x^4 + 2x^3 + x + 4$.
El resto debe ser 1.

$$
\begin{array}{r|ccccccc}
 & 5 & 2 & 0 & 2 & 5 & 5 & 2 \\
-2 = 5 & & & & & & & \\
0 & & & & & & & \\
-1 = 6 & & & & & & & \\
-4 = 3 & & & & & & & \\
\hline
 & & & & & & &
\end{array}
$$

Inversos de polinomios modulares. Ejemplo 1

Sea $A = \mathbb{Z}_7[x]_{x^4+2x^3+x+4}$ y $q(x) = x^3 + 3x^2 + 5x + 2$.
Vamos a calcular, si es posible, $q(x)^{-1}$ (en A).
Ya hemos visto que $q(x)^{-1} = 5x^3 + x^2 + 1$.
Vamos a comprobarlo.
$(x^3 + 3x^2 + 5x + 2) \cdot (5x^3 + x^2 + 1) = 5x^6 + 2x^5 + 2x^3 + 5x^2 + 5x + 2$
Dividimos este polinomio entre $x^4 + 2x^3 + x + 4$.
El resto debe ser 1.

$$\begin{array}{r|ccccccc}
 & 5 & 2 & 0 & 2 & 5 & 5 & 2 \\
5 & & & & & & & \\
0 & & & & & & & \\
6 & & & & & & & \\
3 & & & & & & & \\
\hline
 & 5 & & & & & &
\end{array}$$

Inversos de polinomios modulares. Ejemplo 1

Sea $A = \mathbb{Z}_7[x]_{x^4+2x^3+x+4}$ y $q(x) = x^3 + 3x^2 + 5x + 2$.
Vamos a calcular, si es posible, $q(x)^{-1}$ (en A).
Ya hemos visto que $q(x)^{-1} = 5x^3 + x^2 + 1$.
Vamos a comprobarlo.
$(x^3 + 3x^2 + 5x + 2) \cdot (5x^3 + x^2 + 1) = 5x^6 + 2x^5 + 2x^3 + 5x^2 + 5x + 2$
Dividimos este polinomio entre $x^4 + 2x^3 + x + 4$.
El resto debe ser 1.

$$\begin{array}{c|ccccccc}
 & 5 & 2 & 0 & 2 & 5 & 5 & 2 \\
5 & & 4 & & & & & \\
0 & & & 0 & & & & \\
6 & & & & 2 & & & \\
3 & & & & & 1 & & \\
\hline
 & 5 & & & & & &
\end{array}$$

Inversos de polinomios modulares. Ejemplo 1

Sea $A = \mathbb{Z}_7[x]_{x^4+2x^3+x+4}$ y $q(x) = x^3 + 3x^2 + 5x + 2$.
Vamos a calcular, si es posible, $q(x)^{-1}$ (en A).
Ya hemos visto que $q(x)^{-1} = 5x^3 + x^2 + 1$.
Vamos a comprobarlo.
$(x^3 + 3x^2 + 5x + 2) \cdot (5x^3 + x^2 + 1) = 5x^6 + 2x^5 + 2x^3 + 5x^2 + 5x + 2$
Dividimos este polinomio entre $x^4 + 2x^3 + x + 4$.
El resto debe ser 1.

$$
\begin{array}{c|ccccccc}
 & 5 & 2 & 0 & 2 & 5 & 5 & 2 \\
5 & & 4 & & & & & \\
0 & & & 0 & & & & \\
6 & & & & 2 & & & \\
3 & & & & & 1 & & \\
\hline
 & 5 & 6 & & & & &
\end{array}
$$

Inversos de polinomios modulares. Ejemplo 1

Sea $A = \mathbb{Z}_7[x]_{x^4+2x^3+x+4}$ y $q(x) = x^3 + 3x^2 + 5x + 2$.
Vamos a calcular, si es posible, $q(x)^{-1}$ (en A).
Ya hemos visto que $q(x)^{-1} = 5x^3 + x^2 + 1$.
Vamos a comprobarlo.
$(x^3 + 3x^2 + 5x + 2) \cdot (5x^3 + x^2 + 1) = 5x^6 + 2x^5 + 2x^3 + 5x^2 + 5x + 2$
Dividimos este polinomio entre $x^4 + 2x^3 + x + 4$.
El resto debe ser 1.

$$
\begin{array}{c|ccccccc}
 & 5 & 2 & 0 & 2 & 5 & 5 & 2 \\
5 & & 4 & 2 & & & & \\
0 & & & 0 & 0 & & & \\
6 & & & & 2 & 1 & & \\
3 & & & & & 1 & 4 & \\
\hline
 & 5 & 6 & & & & &
\end{array}
$$

Inversos de polinomios modulares. Ejemplo 1

Sea $A = \mathbb{Z}_7[x]_{x^4+2x^3+x+4}$ y $q(x) = x^3 + 3x^2 + 5x + 2$.
Vamos a calcular, si es posible, $q(x)^{-1}$ (en A).
Ya hemos visto que $q(x)^{-1} = 5x^3 + x^2 + 1$.
Vamos a comprobarlo.
$(x^3 + 3x^2 + 5x + 2) \cdot (5x^3 + x^2 + 1) = 5x^6 + 2x^5 + 2x^3 + 5x^2 + 5x + 2$
Dividimos este polinomio entre $x^4 + 2x^3 + x + 4$.
El resto debe ser 1.

$$
\begin{array}{c|ccccccc}
 & 5 & 2 & 0 & 2 & 5 & 5 & 2 \\
5 & & 4 & 2 & & & & \\
0 & & & 0 & 0 & & & \\
6 & & & & 2 & 1 & & \\
3 & & & & & 1 & 4 & \\
\hline
 & 5 & 6 & 2 & & & &
\end{array}
$$

Inversos de polinomios modulares. Ejemplo 1

Sea $A = \mathbb{Z}_7[x]_{x^4+2x^3+x+4}$ y $q(x) = x^3 + 3x^2 + 5x + 2$.
Vamos a calcular, si es posible, $q(x)^{-1}$ (en A).
Ya hemos visto que $q(x)^{-1} = 5x^3 + x^2 + 1$.
Vamos a comprobarlo.
$(x^3 + 3x^2 + 5x + 2) \cdot (5x^3 + x^2 + 1) = 5x^6 + 2x^5 + 2x^3 + 5x^2 + 5x + 2$
Dividimos este polinomio entre $x^4 + 2x^3 + x + 4$.
El resto debe ser 1.

	5	2	0	2	5	5	2
5		4	2	3			
0			0	0	0		
6				2	1	5	
3					1	4	6
	5	6	2				

Inversos de polinomios modulares. Ejemplo 1

Sea $A = \mathbb{Z}_7[x]_{x^4+2x^3+x+4}$ y $q(x) = x^3 + 3x^2 + 5x + 2$.
Vamos a calcular, si es posible, $q(x)^{-1}$ (en A).
Ya hemos visto que $q(x)^{-1} = 5x^3 + x^2 + 1$.
Vamos a comprobarlo.
$(x^3 + 3x^2 + 5x + 2) \cdot (5x^3 + x^2 + 1) = 5x^6 + 2x^5 + 2x^3 + 5x^2 + 5x + 2$
Dividimos este polinomio entre $x^4 + 2x^3 + x + 4$.
El resto debe ser 1.

	5	2	0	2	5	5	2
5		4	2	3			
0			0	0	0		
6				2	1	5	
3					1	4	6
	5	6	2	0	0	0	1

Inversos de polinomios modulares. Ejemplo 1

Sea $A = \mathbb{Z}_7[x]_{x^4+2x^3+x+4}$ y $q(x) = x^3 + 3x^2 + 5x + 2$.
Vamos a calcular, si es posible, $q(x)^{-1}$ (en A).
Ya hemos visto que $q(x)^{-1} = 5x^3 + x^2 + 1$.
Vamos a comprobarlo.
$(x^3 + 3x^2 + 5x + 2) \cdot (5x^3 + x^2 + 1) = 5x^6 + 2x^5 + 2x^3 + 5x^2 + 5x + 2$
Dividimos este polinomio entre $x^4 + 2x^3 + x + 4$.
El resto debe ser 1.

$$\begin{array}{c|ccccccc}
 & 5 & 2 & 0 & 2 & 5 & 5 & 2 \\
5 & & 4 & 2 & 3 & & & \\
0 & & & 0 & 0 & 0 & & \\
6 & & & & 2 & 1 & 5 & \\
3 & & & & & 1 & 4 & 6 \\
\hline
 & 5 & 6 & 2 & 0 & 0 & 0 & 1
\end{array}$$

$$c(x) = 5x^2 + 6x + 2; \quad r(x) = 1.$$

Inversos modulares de polinomios. Ejemplo 2.

Inversos modulares de polinomios. Ejemplo 2.

Sea ahora $A = \mathbb{Z}_5[x]_{x^4+3x^3+2x^2+x+4}$ y $q(x) = 3x^3 + 4x + 1$.

Sea ahora $A = \mathbb{Z}_5[x]_{x^4+3x^3+2x^2+x+4}$ y $q(x) = 3x^3 + 4x + 1$.
Calculemos en A, si existe, $q(x)^{-1}$.

Inversos modulares de polinomios. Ejemplo 2.

Sea ahora $A = \mathbb{Z}_5[x]_{x^4+3x^3+2x^2+x+4}$ y $q(x) = 3x^3 + 4x + 1$.
Calculemos en A, si existe, $q(x)^{-1}$.
Procedemos igual que en el ejemplo anterior.

Sea ahora $A = \mathbb{Z}_5[x]_{x^4+3x^3+2x^2+x+4}$ y $q(x) = 3x^3 + 4x + 1$.
Calculemos en A, si existe, $q(x)^{-1}$.
Procedemos igual que en el ejemplo anterior.

$x^4 + 3x^3 + 2x^2 + x + 4$	
$3x^3 + 4x + 1$	

Inversos modulares de polinomios. Ejemplo 2.

Sea ahora $A = \mathbb{Z}_5[x]_{x^4+3x^3+2x^2+x+4}$ y $q(x) = 3x^3 + 4x + 1$.
Calculemos en A, si existe, $q(x)^{-1}$.
Procedemos igual que en el ejemplo anterior.

$x^4 + 3x^3 + 2x^2 + x + 4$	
$3x^3 + 4x + 1$	

$x^4 + 3x^3 + 2x^2 + x + 4 = (3x^3 + 4x + 1) \cdot (2x + 1) + (4x^2 + 3)$

Inversos modulares de polinomios. Ejemplo 2.

Sea ahora $A = \mathbb{Z}_5[x]_{x^4+3x^3+2x^2+x+4}$ y $q(x) = 3x^3 + 4x + 1$.
Calculemos en A, si existe, $q(x)^{-1}$.
Procedemos igual que en el ejemplo anterior.

$x^4 + 3x^3 + 2x^2 + x + 4$	
$3x^3 + 4x + 1$	
$4x^2 + 3$	$2x + 1$

$x^4 + 3x^3 + 2x^2 + x + 4 = (3x^3 + 4x + 1) \cdot (2x + 1) + (4x^2 + 3)$

Inversos modulares de polinomios. Ejemplo 2.

Sea ahora $A = \mathbb{Z}_5[x]_{x^4+3x^3+2x^2+x+4}$ y $q(x) = 3x^3 + 4x + 1$.
Calculemos en A, si existe, $q(x)^{-1}$.
Procedemos igual que en el ejemplo anterior.

$x^4 + 3x^3 + 2x^2 + x + 4$	
$3x^3 + 4x + 1$	
$4x^2 + 3$	$2x + 1$

$x^4 + 3x^3 + 2x^2 + x + 4 = (3x^3 + 4x + 1) \cdot (2x + 1) + (4x^2 + 3)$
$3x^3 + 4x + 1 = (4x^2 + 3) \cdot (2x) + (3x + 1)$

Inversos modulares de polinomios. Ejemplo 2.

Sea ahora $A = \mathbb{Z}_5[x]_{x^4+3x^3+2x^2+x+4}$ y $q(x) = 3x^3 + 4x + 1$.
Calculemos en A, si existe, $q(x)^{-1}$.
Procedemos igual que en el ejemplo anterior.

$x^4 + 3x^3 + 2x^2 + x + 4$		
$3x^3 + 4x + 1$		
$4x^2 + 3$	$2x + 1$	$x^4 + 3x^3 + 2x^2 + x + 4 = (3x^3 + 4x + 1) \cdot (2x + 1) + (4x^2 + 3)$
$3x + 1$	$2x$	$3x^3 + 4x + 1 = (4x^2 + 3) \cdot (2x) + (3x + 1)$

Inversos modulares de polinomios. Ejemplo 2.

Sea ahora $A = \mathbb{Z}_5[x]_{x^4+3x^3+2x^2+x+4}$ y $q(x) = 3x^3 + 4x + 1$.
Calculemos en A, si existe, $q(x)^{-1}$.
Procedemos igual que en el ejemplo anterior.

$x^4 + 3x^3 + 2x^2 + x + 4$	
$3x^3 + 4x + 1$	
$4x^2 + 3$	$2x + 1$
$3x + 1$	$2x$

$x^4 + 3x^3 + 2x^2 + x + 4 = (3x^3 + 4x + 1) \cdot (2x + 1) + (4x^2 + 3)$
$3x^3 + 4x + 1 = (4x^2 + 3) \cdot (2x) + (3x + 1)$
$4x^2 + 3 = (3x + 1) \cdot (3x + 4) + (4)$

Inversos modulares de polinomios. Ejemplo 2.

Sea ahora $A = \mathbb{Z}_5[x]_{x^4+3x^3+2x^2+x+4}$ y $q(x) = 3x^3 + 4x + 1$.
Calculemos en A, si existe, $q(x)^{-1}$.
Procedemos igual que en el ejemplo anterior.

$x^4 + 3x^3 + 2x^2 + x + 4$		
$3x^3 + 4x + 1$		
$4x^2 + 3$	$2x + 1$	$x^4 + 3x^3 + 2x^2 + x + 4 = (3x^3 + 4x + 1) \cdot (2x + 1) + (4x^2 + 3)$
$3x + 1$	$2x$	$3x^3 + 4x + 1 = (4x^2 + 3) \cdot (2x) + (3x + 1)$
4	$3x + 4$	$4x^2 + 3 = (3x + 1) \cdot (3x + 4) + (4)$

Inversos modulares de polinomios. Ejemplo 2.

Sea ahora $A = \mathbb{Z}_5[x]_{x^4+3x^3+2x^2+x+4}$ y $q(x) = 3x^3 + 4x + 1$.
Calculemos en A, si existe, $q(x)^{-1}$.
Procedemos igual que en el ejemplo anterior.

$x^4 + 3x^3 + 2x^2 + x + 4$		
$3x^3 + 4x + 1$		
$4x^2 + 3$	$2x + 1$	$x^4 + 3x^3 + 2x^2 + x + 4 = (3x^3 + 4x + 1) \cdot (2x + 1) + (4x^2 + 3)$
$3x + 1$	$2x$	$3x^3 + 4x + 1 = (4x^2 + 3) \cdot (2x) + (3x + 1)$
4	$3x + 4$	$4x^2 + 3 = (3x + 1) \cdot (3x + 4) + (4)$

Y puesto que $3x + 1 = 4 \cdot (2x + 4) + 0$, ya hemos terminado con las divisiones (el resto de la siguiente división sería cero).

Inversos modulares de polinomios. Ejemplo 2.

Sea ahora $A = \mathbb{Z}_5[x]_{x^4+3x^3+2x^2+x+4}$ y $q(x) = 3x^3 + 4x + 1$.
Calculemos en A, si existe, $q(x)^{-1}$.
Procedemos igual que en el ejemplo anterior.

$x^4 + 3x^3 + 2x^2 + x + 4$		
$3x^3 + 4x + 1$		
$4x^2 + 3$	$2x + 1$	$x^4 + 3x^3 + 2x^2 + x + 4 = (3x^3 + 4x + 1) \cdot (2x + 1) + (4x^2 + 3)$
$3x + 1$	$2x$	$3x^3 + 4x + 1 = (4x^2 + 3) \cdot (2x) + (3x + 1)$
4	$3x + 4$	$4x^2 + 3 = (3x + 1) \cdot (3x + 4) + (4)$

El resto de la última división no es un polinomio mónico (su coeficiente líder es 4).

Inversos modulares de polinomios. Ejemplo 2.

Sea ahora $A = \mathbb{Z}_5[x]_{x^4+3x^3+2x^2+x+4}$ y $q(x) = 3x^3 + 4x + 1$.
Calculemos en A, si existe, $q(x)^{-1}$.
Procedemos igual que en el ejemplo anterior.

$x^4 + 3x^3 + 2x^2 + x + 4$		
$3x^3 + 4x + 1$		
$4x^2 + 3$	$2x + 1$	$x^4 + 3x^3 + 2x^2 + x + 4 = (3x^3 + 4x + 1) \cdot (2x + 1) + (4x^2 + 3)$
$3x + 1$	$2x$	$3x^3 + 4x + 1 = (4x^2 + 3) \cdot (2x) + (3x + 1)$
4	$3x + 4$	$4x^2 + 3 = (3x + 1) \cdot (3x + 4) + (4)$

El resto de la última división no es un polinomio mónico (su coeficiente líder es 4).
Para calcular el máximo común divisor hay que multiplicar por el inverso del coeficiente líder.

Inversos modulares de polinomios. Ejemplo 2.

Sea ahora $A = \mathbb{Z}_5[x]_{x^4+3x^3+2x^2+x+4}$ y $q(x) = 3x^3 + 4x + 1$.
Calculemos en A, si existe, $q(x)^{-1}$.
Procedemos igual que en el ejemplo anterior.

$x^4 + 3x^3 + 2x^2 + x + 4$		
$3x^3 + 4x + 1$		
$4x^2 + 3$	$2x + 1$	$x^4 + 3x^3 + 2x^2 + x + 4 = (3x^3 + 4x + 1) \cdot (2x + 1) + (4x^2 + 3)$
$3x + 1$	$2x$	$3x^3 + 4x + 1 = (4x^2 + 3) \cdot (2x) + (3x + 1)$
4	$3x + 4$	$4x^2 + 3 = (3x + 1) \cdot (3x + 4) + (4)$

El resto de la última división no es un polinomio mónico (su coeficiente líder es 4).
Para calcular el máximo común divisor hay que multiplicar por el inverso del coeficiente líder.
Puesto que $4^{-1} = 4$, multiplicamos por 4, y nos que da 1.

Inversos modulares de polinomios. Ejemplo 2.

Sea ahora $A = \mathbb{Z}_5[x]_{x^4+3x^3+2x^2+x+4}$ y $q(x) = 3x^3 + 4x + 1$.
Calculemos en A, si existe, $q(x)^{-1}$.
Procedemos igual que en el ejemplo anterior.

$x^4 + 3x^3 + 2x^2 + x + 4$		
$3x^3 + 4x + 1$		
$4x^2 + 3$	$2x + 1$	$x^4 + 3x^3 + 2x^2 + x + 4 = (3x^3 + 4x + 1) \cdot (2x + 1) + (4x^2 + 3)$
$3x + 1$	$2x$	$3x^3 + 4x + 1 = (4x^2 + 3) \cdot (2x) + (3x + 1)$
4	$3x + 4$	$4x^2 + 3 = (3x + 1) \cdot (3x + 4) + (4)$

El resto de la última división no es un polinomio mónico (su coeficiente líder es 4).
Para calcular el máximo común divisor hay que multiplicar por el inverso del coeficiente líder.
Puesto que $4^{-1} = 4$, multiplicamos por 4, y nos que da 1.
Por tanto, $\text{mcd}(x^4 + 3x^3 + 2x^2 + x + 4, 3x^3 + 4x + 1) = 1$, y el inverso existe.

Inversos modulares de polinomios. Ejemplo 2.

Sea ahora $A = \mathbb{Z}_5[x]_{x^4+3x^3+2x^2+x+4}$ y $q(x) = 3x^3 + 4x + 1$.
Calculemos en A, si existe, $q(x)^{-1}$.
Procedemos igual que en el ejemplo anterior.

$x^4 + 3x^3 + 2x^2 + x + 4$		
$3x^3 + 4x + 1$		
$4x^2 + 3$	$2x + 1$	$x^4 + 3x^3 + 2x^2 + x + 4 = (3x^3 + 4x + 1) \cdot (2x + 1) + (4x^2 + 3)$
$3x + 1$	$2x$	$3x^3 + 4x + 1 = (4x^2 + 3) \cdot (2x) + (3x + 1)$
4	$3x + 4$	$4x^2 + 3 = (3x + 1) \cdot (3x + 4) + (4)$

El resto de la última división no es un polinomio mónico (su coeficiente líder es 4).
Para calcular el máximo común divisor hay que multiplicar por el inverso del coeficiente líder.
Puesto que $4^{-1} = 4$, multiplicamos por 4, y nos que da 1.
Por tanto, $\mathrm{mcd}(x^4 + 3x^3 + 2x^2 + x + 4, 3x^3 + 4x + 1) = 1$, y el inverso existe.
Añadimos una fila al final y una columna a la derecha para realizar el cálculo.

Inversos modulares de polinomios. Ejemplo 2.

Sea ahora $A = \mathbb{Z}_5[x]_{x^4+3x^3+2x^2+x+4}$ y $q(x) = 3x^3 + 4x + 1$.
Calculemos en A, si existe, $q(x)^{-1}$.
Procedemos igual que en el ejemplo anterior.

$x^4 + 3x^3 + 2x^2 + x + 4$		0
$3x^3 + 4x + 1$		1
$4x^2 + 3$	$2x + 1$	$v_1(x)$
$3x + 1$	$2x$	$v_2(x)$
4	$3x + 4$	$v_3(x)$
1		$4 \cdot v_3(x)$

Inversos modulares de polinomios. Ejemplo 2.

Sea ahora $A = \mathbb{Z}_5[x]_{x^4+3x^3+2x^2+x+4}$ y $q(x) = 3x^3 + 4x + 1$.
Calculemos en A, si existe, $q(x)^{-1}$.
Procedemos igual que en el ejemplo anterior.

$x^4 + 3x^3 + 2x^2 + x + 4$		0
$3x^3 + 4x + 1$		1
$4x^2 + 3$	$2x + 1$	$v_1(x)$
$3x + 1$	$2x$	$v_2(x)$
4	$3x + 4$	$v_3(x)$
1		$4 \cdot v_3(x)$

$v_1(x) = 0 - (2x + 1) \cdot 1 = 3x + 4$

Inversos modulares de polinomios. Ejemplo 2.

Sea ahora $A = \mathbb{Z}_5[x]_{x^4+3x^3+2x^2+x+4}$ y $q(x) = 3x^3 + 4x + 1$.
Calculemos en A, si existe, $q(x)^{-1}$.
Procedemos igual que en el ejemplo anterior.

$x^4 + 3x^3 + 2x^2 + x + 4$		0
$3x^3 + 4x + 1$		1
$4x^2 + 3$	$2x + 1$	$3x + 4$
$3x + 1$	$2x$	$v_2(x)$
4	$3x + 4$	$v_3(x)$
1		$4 \cdot v_3(x)$

$$v_1(x) = 0 - (2x + 1) \cdot 1 = 3x + 4$$

Inversos modulares de polinomios. Ejemplo 2.

Sea ahora $A = \mathbb{Z}_5[x]_{x^4+3x^3+2x^2+x+4}$ y $q(x) = 3x^3 + 4x + 1$.
Calculemos en A, si existe, $q(x)^{-1}$.
Procedemos igual que en el ejemplo anterior.

$x^4 + 3x^3 + 2x^2 + x + 4$		0
$3x^3 + 4x + 1$		1
$4x^2 + 3$	$2x + 1$	$3x + 4$
$3x + 1$	$2x$	$v_2(x)$
4	$3x + 4$	$v_3(x)$
1		$4 \cdot v_3(x)$

$v_1(x) = 0 - (2x + 1) \cdot 1 = 3x + 4$
$v_2(x) = 1 - 2x \cdot (3x + 4) = 4x^2 + 2x + 1$

Inversos modulares de polinomios. Ejemplo 2.

Sea ahora $A = \mathbb{Z}_5[x]_{x^4+3x^3+2x^2+x+4}$ y $q(x) = 3x^3 + 4x + 1$.
Calculemos en A, si existe, $q(x)^{-1}$.
Procedemos igual que en el ejemplo anterior.

$x^4 + 3x^3 + 2x^2 + x + 4$		0
$3x^3 + 4x + 1$		1
$4x^2 + 3$	$2x + 1$	$3x + 4$
$3x + 1$	$2x$	$4x^2 + 2x + 1$
4	$3x + 4$	$v_3(x)$
1		$4 \cdot v_3(x)$

$v_1(x) = 0 - (2x + 1) \cdot 1 = 3x + 4$
$v_2(x) = 1 - 2x \cdot (3x + 4) = 4x^2 + 2x + 1$

Inversos modulares de polinomios. Ejemplo 2.

Sea ahora $A = \mathbb{Z}_5[x]_{x^4+3x^3+2x^2+x+4}$ y $q(x) = 3x^3 + 4x + 1$.
Calculemos en A, si existe, $q(x)^{-1}$.
Procedemos igual que en el ejemplo anterior.

$x^4 + 3x^3 + 2x^2 + x + 4$		0
$3x^3 + 4x + 1$		1
$4x^2 + 3$	$2x + 1$	$3x + 4$
$3x + 1$	$2x$	$4x^2 + 2x + 1$
4	$3x + 4$	$v_3(x)$
1		$4 \cdot v_3(x)$

$v_1(x) = 0 - (2x + 1) \cdot 1 = 3x + 4$
$v_2(x) = 1 - 2x \cdot (3x + 4) = 4x^2 + 2x + 1$
$v_3(x) = 3x + 4 - (3x + 4) \cdot (4x^2 + 2x + 1)$

Inversos modulares de polinomios. Ejemplo 2.

Sea ahora $A = \mathbb{Z}_5[x]_{x^4+3x^3+2x^2+x+4}$ y $q(x) = 3x^3 + 4x + 1$.
Calculemos en A, si existe, $q(x)^{-1}$.
Procedemos igual que en el ejemplo anterior.

$x^4 + 3x^3 + 2x^2 + x + 4$		0
$3x^3 + 4x + 1$		1
$4x^2 + 3$	$2x + 1$	$3x + 4$
$3x + 1$	$2x$	$4x^2 + 2x + 1$
4	$3x + 4$	$v_3(x)$
1		$4 \cdot v_3(x)$

$$
\begin{aligned}
v_1(x) &= 0 - (2x+1)\cdot 1 = 3x + 4 \\
v_2(x) &= 1 - 2x \cdot (3x+4) = 4x^2 + 2x + 1 \\
v_3(x) &= 3x + 4 - (3x+4)\cdot(4x^2 + 2x + 1) \\
&= 3x^3 + 3x^2 + 2x
\end{aligned}
$$

Inversos modulares de polinomios. Ejemplo 2.

Sea ahora $A = \mathbb{Z}_5[x]_{x^4+3x^3+2x^2+x+4}$ y $q(x) = 3x^3 + 4x + 1$.
Calculemos en A, si existe, $q(x)^{-1}$.
Procedemos igual que en el ejemplo anterior.

$x^4 + 3x^3 + 2x^2 + x + 4$		0
$3x^3 + 4x + 1$		1
$4x^2 + 3$	$2x + 1$	$3x + 4$
$3x + 1$	$2x$	$4x^2 + 2x + 1$
4	$3x + 4$	$3x^3 + 3x^2 + 2x$
1		$4 \cdot v_3(x)$

$v_1(x) = 0 - (2x + 1) \cdot 1 = 3x + 4$
$v_2(x) = 1 - 2x \cdot (3x + 4) = 4x^2 + 2x + 1$
$v_3(x) = 3x^3 + 3x^2 + 2x$

Inversos modulares de polinomios. Ejemplo 2.

Sea ahora $A = \mathbb{Z}_5[x]_{x^4+3x^3+2x^2+x+4}$ y $q(x) = 3x^3 + 4x + 1$.
Calculemos en A, si existe, $q(x)^{-1}$.
Procedemos igual que en el ejemplo anterior.

$x^4 + 3x^3 + 2x^2 + x + 4$		0
$3x^3 + 4x + 1$		1
$4x^2 + 3$	$2x + 1$	$3x + 4$
$3x + 1$	$2x$	$4x^2 + 2x + 1$
4	$3x + 4$	$3x^3 + 3x^2 + 2x$
1		$4 \cdot v_3(x)$

$v_1(x) = 0 - (2x + 1) \cdot 1 = 3x + 4$
$v_2(x) = 1 - 2x \cdot (3x + 4) = 4x^2 + 2x + 1$
$v_3(x) = 3x^3 + 3x^2 + 2x$

$4 \cdot v_3(x) = 2x^3 + 2x^2 + 3x$

Inversos modulares de polinomios. Ejemplo 2.

Sea ahora $A = \mathbb{Z}_5[x]_{x^4+3x^3+2x^2+x+4}$ y $q(x) = 3x^3 + 4x + 1$.
Calculemos en A, si existe, $q(x)^{-1}$.
Procedemos igual que en el ejemplo anterior.

$x^4 + 3x^3 + 2x^2 + x + 4$		0
$3x^3 + 4x + 1$		1
$4x^2 + 3$	$2x + 1$	$3x + 4$
$3x + 1$	$2x$	$4x^2 + 2x + 1$
4	$3x + 4$	$3x^3 + 3x^2 + 2x$
1		$2x^3 + 2x^2 + 3x$

$v_1(x) = 0 - (2x + 1) \cdot 1 = 3x + 4$
$v_2(x) = 1 - 2x \cdot (3x + 4) = 4x^2 + 2x + 1$
$v_3(x) = 3x^3 + 3x^2 + 2x$

$4 \cdot v_3(x) = 2x^3 + 2x^2 + 3x$

Inversos modulares de polinomios. Ejemplo 2.

Sea ahora $A = \mathbb{Z}_5[x]_{x^4+3x^3+2x^2+x+4}$ y $q(x) = 3x^3 + 4x + 1$.
Calculemos en A, si existe, $q(x)^{-1}$.
Procedemos igual que en el ejemplo anterior.

$x^4 + 3x^3 + 2x^2 + x + 4$		0
$3x^3 + 4x + 1$		1
$4x^2 + 3$	$2x + 1$	$3x + 4$
$3x + 1$	$2x$	$4x^2 + 2x + 1$
4	$3x + 4$	$3x^3 + 3x^2 + 2x$
1		$2x^3 + 2x^2 + 3x$

$v_1(x) = 0 - (2x + 1) \cdot 1 = 3x + 4$
$v_2(x) = 1 - 2x \cdot (3x + 4) = 4x^2 + 2x + 1$
$v_3(x) = 3x^3 + 3x^2 + 2x$
$4 \cdot v_3(x) = 2x^3 + 2x^2 + 3x$

El resultado final es:

Inversos modulares de polinomios. Ejemplo 2.

Sea ahora $A = \mathbb{Z}_5[x]_{x^4+3x^3+2x^2+x+4}$ y $q(x) = 3x^3 + 4x + 1$.
Calculemos en A, si existe, $q(x)^{-1}$.
Procedemos igual que en el ejemplo anterior.

$x^4 + 3x^3 + 2x^2 + x + 4$		0
$3x^3 + 4x + 1$		1
$4x^2 + 3$	$2x + 1$	$3x + 4$
$3x + 1$	$2x$	$4x^2 + 2x + 1$
4	$3x + 4$	$3x^3 + 3x^2 + 2x$
1		$2x^3 + 2x^2 + 3x$

$v_1(x) = 0 - (2x + 1) \cdot 1 = 3x + 4$
$v_2(x) = 1 - 2x \cdot (3x + 4) = 4x^2 + 2x + 1$
$v_3(x) = 3x^3 + 3x^2 + 2x$
$4 \cdot v_3(x) = 2x^3 + 2x^2 + 3x$

El resultado final es:

$$q(x)^{-1} = 2x^3 + 2x^2 + 3x.$$

Inversos modulares de polinomios. Ejemplo 3.

Inversos modulares de polinomios. Ejemplo 3.

En $\mathbb{Z}_3[x]_{x^4+2x^3+2x^2+2x+2}$ vamos a calcular, si es posible, $(x^3+x+1)^{-1}$.

Inversos modulares de polinomios. Ejemplo 3.

En $\mathbb{Z}_3[x]_{x^4+2x^3+2x^2+2x+2}$ vamos a calcular, si es posible, $(x^3+x+1)^{-1}$.
En primer lugar calculamos $\mathrm{mcd}(x^4+2x^3+2x^2+2x+2, x^3+x+1)$.

Inversos modulares de polinomios. Ejemplo 3.

En $\mathbb{Z}_3[x]_{x^4+2x^3+2x^2+2x+2}$ vamos a calcular, si es posible, $(x^3+x+1)^{-1}$.
En primer lugar calculamos $\mathrm{mcd}(x^4+2x^3+2x^2+2x+2, x^3+x+1)$.

$$x^4+2x^3+2x^2+2x+2 = (x^3+x+1)\cdot(x+2)+(x^2+2x).$$

Inversos modulares de polinomios. Ejemplo 3.

En $\mathbb{Z}_3[x]_{x^4+2x^3+2x^2+2x+2}$ vamos a calcular, si es posible, $(x^3+x+1)^{-1}$.
En primer lugar calculamos $\mathrm{mcd}(x^4+2x^3+2x^2+2x+2, x^3+x+1)$.

$$x^4+2x^3+2x^2+2x+2=(x^3+x+1)\cdot(x+2)+(x^2+2x).$$
$$x^3+x+1=(x^2+2x)\cdot(x+1)+(2x+1).$$

Inversos modulares de polinomios. Ejemplo 3.

En $\mathbb{Z}_3[x]_{x^4+2x^3+2x^2+2x+2}$ vamos a calcular, si es posible, $(x^3+x+1)^{-1}$.
En primer lugar calculamos $\mathrm{mcd}(x^4+2x^3+2x^2+2x+2, x^3+x+1)$.

$$x^4+2x^3+2x^2+2x+2 = (x^3+x+1)\cdot(x+2)+(x^2+2x).$$
$$x^3+x+1 = (x^2+2x)\cdot(x+1)+(2x+1).$$
$$x^2+2x = (2x+1)\cdot(2x)+0.$$

Inversos modulares de polinomios. Ejemplo 3.

En $\mathbb{Z}_3[x]_{x^4+2x^3+2x^2+2x+2}$ vamos a calcular, si es posible, $(x^3+x+1)^{-1}$.
En primer lugar calculamos $\text{mcd}(x^4+2x^3+2x^2+2x+2, x^3+x+1)$.

$$x^4+2x^3+2x^2+2x+2 = (x^3+x+1)\cdot(x+2)+(x^2+2x).$$
$$x^3+x+1 = (x^2+2x)\cdot(x+1)+(2x+1).$$
$$x^2+2x = (2x+1)\cdot(2x)+0.$$

El último resto distinto de cero es $2x+1$.

Inversos modulares de polinomios. Ejemplo 3.

En $\mathbb{Z}_3[x]_{x^4+2x^3+2x^2+2x+2}$ vamos a calcular, si es posible, $(x^3+x+1)^{-1}$.
En primer lugar calculamos $\mathrm{mcd}(x^4+2x^3+2x^2+2x+2, x^3+x+1)$.

$$x^4+2x^3+2x^2+2x+2 = (x^3+x+1)\cdot(x+2)+(x^2+2x).$$
$$x^3+x+1 = (x^2+2x)\cdot(x+1)+(2x+1).$$
$$x^2+2x = (2x+1)\cdot(2x)+0.$$

El último resto distinto de cero es $2x+1$.
Este polinomio no es mónico. Su coeficiente líder es 2.

Inversos modulares de polinomios. Ejemplo 3.

En $\mathbb{Z}_3[x]_{x^4+2x^3+2x^2+2x+2}$ vamos a calcular, si es posible, $(x^3+x+1)^{-1}$.
En primer lugar calculamos $\mathrm{mcd}(x^4+2x^3+2x^2+2x+2, x^3+x+1)$.

$$x^4+2x^3+2x^2+2x+2 = (x^3+x+1)\cdot(x+2)+(x^2+2x).$$
$$x^3+x+1 = (x^2+2x)\cdot(x+1)+(2x+1).$$
$$x^2+2x = (2x+1)\cdot(2x)+0.$$

El último resto distinto de cero es $2x+1$.
Este polinomio no es mónico. Su coeficiente líder es 2.
Puesto que $2^{-1}=2$, multiplicamos este polinomio por 2.

Inversos modulares de polinomios. Ejemplo 3.

En $\mathbb{Z}_3[x]_{x^4+2x^3+2x^2+2x+2}$ vamos a calcular, si es posible, $(x^3+x+1)^{-1}$.
En primer lugar calculamos $\mathrm{mcd}(x^4+2x^3+2x^2+2x+2, x^3+x+1)$.

$$x^4+2x^3+2x^2+2x+2 = (x^3+x+1)\cdot(x+2)+(x^2+2x).$$
$$x^3+x+1 = (x^2+2x)\cdot(x+1)+(2x+1).$$
$$x^2+2x = (2x+1)\cdot(2x)+0.$$

El último resto distinto de cero es $2x+1$.
Este polinomio no es mónico. Su coeficiente líder es 2.
Puesto que $2^{-1}=2$, multiplicamos este polinomio por 2.
El resultado de esta multiplicación, que es $x+2$, es el máximo común divisor que buscábamos.

Inversos modulares de polinomios. Ejemplo 3.

En $\mathbb{Z}_3[x]_{x^4+2x^3+2x^2+2x+2}$ vamos a calcular, si es posible, $(x^3+x+1)^{-1}$.
En primer lugar calculamos $\mathrm{mcd}(x^4+2x^3+2x^2+2x+2, x^3+x+1)$.

$$x^4+2x^3+2x^2+2x+2 = (x^3+x+1)\cdot(x+2)+(x^2+2x).$$
$$x^3+x+1 = (x^2+2x)\cdot(x+1)+(2x+1).$$
$$x^2+2x = (2x+1)\cdot(2x)+0.$$

El último resto distinto de cero es $2x+1$.
Este polinomio no es mónico. Su coeficiente líder es 2.
Puesto que $2^{-1}=2$, multiplicamos este polinomio por 2.
El resultado de esta multiplicación, que es $x+2$, es el máximo común divisor que buscábamos.
Puesto que $\mathrm{mcd}(x^4+2x^3+2x^2+2x+2, x^3+x+1) = x+2 \neq 1$ no existe el inverso de x^3+x+1.

Inversos modulares de polinomios. Ejemplo 4.

Inversos modulares de polinomios. Ejemplo 4.

Vamos a tomar por último $A = \mathbb{R}[x]_{x^2+1}$.

Inversos modulares de polinomios. Ejemplo 4.

Vamos a tomar por último $A = \mathbb{R}[x]_{x^2+1}$.
Aquí vamos a calcular $(2x+1)^{-1}$.

Inversos modulares de polinomios. Ejemplo 4.

Vamos a tomar por último $A = \mathbb{R}[x]_{x^2+1}$.
Aquí vamos a calcular $(2x+1)^{-1}$.
Dividimos x^2+1 entre $2x+1$.

Inversos modulares de polinomios. Ejemplo 4.

Vamos a tomar por último $A = \mathbb{R}[x]_{x^2+1}$.
Aquí vamos a calcular $(2x+1)^{-1}$.
Dividimos x^2+1 entre $2x+1$.

$$\begin{array}{r|rrr}
\frac{1}{2} & 1 & 0 & 1 \\
\hline
\frac{-1}{2} & & & \\
\hline
& & &
\end{array}$$

Inversos modulares de polinomios. Ejemplo 4.

Vamos a tomar por último $A = \mathbb{R}[x]_{x^2+1}$.
Aquí vamos a calcular $(2x+1)^{-1}$.
Dividimos x^2+1 entre $2x+1$.

$$\begin{array}{c|ccc}
\frac{1}{2} & 1 & 0 & 1 \\
\hline
\frac{-1}{2} & & & \\
\hline
 & 1 & &
\end{array}$$

Inversos modulares de polinomios. Ejemplo 4.

Vamos a tomar por último $A = \mathbb{R}[x]_{x^2+1}$.
Aquí vamos a calcular $(2x+1)^{-1}$.
Dividimos x^2+1 entre $2x+1$.

$$\begin{array}{c|ccc}
\frac{1}{2} & 1 & 0 & 1 \\
\hline
\frac{-1}{2} & & \frac{-1}{2} & \\
\hline
 & 1 & &
\end{array}$$

Inversos modulares de polinomios. Ejemplo 4.

Vamos a tomar por último $A = \mathbb{R}[x]_{x^2+1}$.
Aquí vamos a calcular $(2x+1)^{-1}$.
Dividimos x^2+1 entre $2x+1$.

$$\begin{array}{c|ccc}
\frac{1}{2} & 1 & 0 & 1 \\
\cline{1-1}
\frac{-1}{2} & & \frac{-1}{2} & \\
\hline
 & 1 & \frac{-1}{2} &
\end{array}$$

Inversos modulares de polinomios. Ejemplo 4.

Vamos a tomar por último $A = \mathbb{R}[x]_{x^2+1}$.
Aquí vamos a calcular $(2x+1)^{-1}$.
Dividimos x^2+1 entre $2x+1$.

$$
\begin{array}{r|ccc}
\frac{1}{2} & 1 & 0 & 1 \\
\hline
 & & & \\
\frac{-1}{2} & & \frac{-1}{2} & \frac{1}{4} \\
 & & & \\
\hline
 & 1 & \frac{-1}{2} &
\end{array}
$$

Inversos modulares de polinomios. Ejemplo 4.

Vamos a tomar por último $A = \mathbb{R}[x]_{x^2+1}$.
Aquí vamos a calcular $(2x+1)^{-1}$.
Dividimos $x^2 + 1$ entre $2x + 1$.

$$\begin{array}{r|ccc}
\frac{1}{2} & 1 & 0 & 1 \\
\hline
\frac{-1}{2} & & \frac{-1}{2} & \frac{1}{4} \\
\hline
 & 1 & \frac{-1}{2} & \frac{5}{4}
\end{array}$$

Inversos modulares de polinomios. Ejemplo 4.

Vamos a tomar por último $A = \mathbb{R}[x]_{x^2+1}$.
Aquí vamos a calcular $(2x+1)^{-1}$.
Dividimos x^2+1 entre $2x+1$.

$$\begin{array}{r|rrr} \frac{1}{2} & 1 & 0 & 1 \\ \hline \frac{-1}{2} & & \frac{-1}{2} & \frac{1}{4} \\ \hline & 1 & \frac{-1}{2} & \frac{5}{4} \end{array}$$

$$c(x) = \frac{1}{2} \cdot \left(x - \frac{1}{2}\right) = \frac{1}{2}x - \frac{1}{4} = \frac{2x-1}{4}; \qquad r(x) = \frac{5}{4}.$$

Inversos modulares de polinomios. Ejemplo 4.

Vamos a tomar por último $A = \mathbb{R}[x]_{x^2+1}$.
Aquí vamos a calcular $(2x+1)^{-1}$.
Dividimos x^2+1 entre $2x+1$.
El cociente es $\frac{2x-1}{4}$ y el resto $\frac{5}{4}$.

Inversos modulares de polinomios. Ejemplo 4.

Vamos a tomar por último $A = \mathbb{R}[x]_{x^2+1}$.
Aquí vamos a calcular $(2x+1)^{-1}$.
Dividimos x^2+1 entre $2x+1$.
El cociente es $\frac{2x-1}{4}$ y el resto $\frac{5}{4}$.
El resto de la siguiente división es 0.

Inversos modulares de polinomios. Ejemplo 4.

Vamos a tomar por último $A = \mathbb{R}[x]_{x^2+1}$.
Aquí vamos a calcular $(2x+1)^{-1}$.
Dividimos x^2+1 entre $2x+1$.
El cociente es $\frac{2x-1}{4}$ y el resto $\frac{5}{4}$.
El resto de la siguiente división es 0.
Puesto que $\frac{5}{4}$ no es mónico, multiplicamos por $\frac{4}{5}$ para que lo sea.

Inversos modulares de polinomios. Ejemplo 4.

Vamos a tomar por último $A = \mathbb{R}[x]_{x^2+1}$.
Aquí vamos a calcular $(2x+1)^{-1}$.
Dividimos x^2+1 entre $2x+1$.
El cociente es $\frac{2x-1}{4}$ y el resto $\frac{5}{4}$.
El resto de la siguiente división es 0.
Puesto que $\frac{5}{4}$ no es mónico, multiplicamos por $\frac{4}{5}$ para que lo sea.

x^2+1		0
$2x+1$		1
$\frac{5}{4}$	$\frac{2x-1}{4}$	
1		

Inversos modulares de polinomios. Ejemplo 4.

Vamos a tomar por último $A = \mathbb{R}[x]_{x^2+1}$.
Aquí vamos a calcular $(2x+1)^{-1}$.
Dividimos x^2+1 entre $2x+1$.
El cociente es $\frac{2x-1}{4}$ y el resto $\frac{5}{4}$.
El resto de la siguiente división es 0.
Puesto que $\frac{5}{4}$ no es mónico, multiplicamos por $\frac{4}{5}$ para que lo sea.

x^2+1		0
$2x+1$		1
$\frac{5}{4}$	$\frac{2x-1}{4}$	
1		

$0 - \frac{2x-1}{4} \cdot 1 = \frac{-2x+1}{4}$.

Inversos modulares de polinomios. Ejemplo 4.

Vamos a tomar por último $A = \mathbb{R}[x]_{x^2+1}$.
Aquí vamos a calcular $(2x+1)^{-1}$.
Dividimos x^2+1 entre $2x+1$.
El cociente es $\frac{2x-1}{4}$ y el resto $\frac{5}{4}$.
El resto de la siguiente división es 0.
Puesto que $\frac{5}{4}$ no es mónico, multiplicamos por $\frac{4}{5}$ para que lo sea.

x^2+1		0
$2x+1$		1
$\frac{5}{4}$	$\frac{2x-1}{4}$	$\frac{-2x+1}{4}$
1		

Inversos modulares de polinomios. Ejemplo 4.

Vamos a tomar por último $A = \mathbb{R}[x]_{x^2+1}$.
Aquí vamos a calcular $(2x+1)^{-1}$.
Dividimos x^2+1 entre $2x+1$.
El cociente es $\frac{2x-1}{4}$ y el resto $\frac{5}{4}$.
El resto de la siguiente división es 0.
Puesto que $\frac{5}{4}$ no es mónico, multiplicamos por $\frac{4}{5}$ para que lo sea.

x^2+1		0
$2x+1$		1
$\frac{5}{4}$	$\frac{2x-1}{4}$	$\frac{-2x+1}{4}$
1		

$\frac{-2x+1}{4} \cdot \frac{4}{5} = \frac{-2x+1}{5} = \frac{1-2x}{5}$.

Inversos modulares de polinomios. Ejemplo 4.

Vamos a tomar por último $A = \mathbb{R}[x]_{x^2+1}$.
Aquí vamos a calcular $(2x+1)^{-1}$.
Dividimos x^2+1 entre $2x+1$.
El cociente es $\frac{2x-1}{4}$ y el resto $\frac{5}{4}$.
El resto de la siguiente división es 0.
Puesto que $\frac{5}{4}$ no es mónico, multiplicamos por $\frac{4}{5}$ para que lo sea.

x^2+1		0
$2x+1$		1
$\frac{5}{4}$	$\frac{2x-1}{4}$	$\frac{-2x+1}{4}$
1		$\frac{1-2x}{5}$

Inversos modulares de polinomios. Ejemplo 4.

Vamos a tomar por último $A = \mathbb{R}[x]_{x^2+1}$.
Aquí vamos a calcular $(2x+1)^{-1}$.
Dividimos x^2+1 entre $2x+1$.
Este inverso ya está calculado y vale $\frac{1-2x}{5}$.

Inversos modulares de polinomios. Ejemplo 4.

Vamos a tomar por último $A = \mathbb{R}[x]_{x^2+1}$.
Aquí vamos a calcular $(2x+1)^{-1}$.
Dividimos x^2+1 entre $2x+1$.
Este inverso ya está calculado y vale $\frac{1-2x}{5}$.
Veamos otra forma de haber calculado este inverso.

Inversos modulares de polinomios. Ejemplo 4.

Vamos a tomar por último $A = \mathbb{R}[x]_{x^2+1}$.
Aquí vamos a calcular $(2x+1)^{-1}$.
Dividimos x^2+1 entre $2x+1$.
Este inverso ya está calculado y vale $\frac{1-2x}{5}$.
Veamos otra forma de haber calculado este inverso.
Notemos que en A, $x^2 = -1$, ya que al dividir x^2 entre x^2+1 el resto es -1.

Inversos modulares de polinomios. Ejemplo 4.

Vamos a tomar por último $A = \mathbb{R}[x]_{x^2+1}$.
Aquí vamos a calcular $(2x+1)^{-1}$.
Dividimos x^2+1 entre $2x+1$.
Este inverso ya está calculado y vale $\frac{1-2x}{5}$.
Veamos otra forma de haber calculado este inverso.
Notemos que en A, $x^2 = -1$, ya que al dividir x^2 entre x^2+1 el resto es -1.
Escribiremos entonces i en lugar de x (se tiene que $i^2 = -1$).

Inversos modulares de polinomios. Ejemplo 4.

Vamos a tomar por último $A = \mathbb{R}[x]_{x^2+1}$.
Aquí vamos a calcular $(2x+1)^{-1}$.
Dividimos x^2+1 entre $2x+1$.
Este inverso ya está calculado y vale $\frac{1-2x}{5}$.
Veamos otra forma de haber calculado este inverso.
Notemos que en A, $x^2 = -1$, ya que al dividir x^2 entre x^2+1 el resto es -1.
Escribiremos entonces i en lugar de x (se tiene que $i^2 = -1$).
Calculamos $(1+2i)^{-1} = \frac{1}{1+2i}$.

Vamos a tomar por último $A = \mathbb{R}[x]_{x^2+1}$.
Aquí vamos a calcular $(2x+1)^{-1}$.
Dividimos x^2+1 entre $2x+1$.
Este inverso ya está calculado y vale $\frac{1-2x}{5}$.
Veamos otra forma de haber calculado este inverso.
Notemos que en A, $x^2 = -1$, ya que al dividir x^2 entre x^2+1 el resto es -1.
Escribiremos entonces i en lugar de x (se tiene que $i^2 = -1$).
Calculamos $(1+2i)^{-1} = \frac{1}{1+2i}$.

$$\frac{1}{1+2i}$$

Inversos modulares de polinomios. Ejemplo 4.

Vamos a tomar por último $A = \mathbb{R}[x]_{x^2+1}$.
Aquí vamos a calcular $(2x+1)^{-1}$.
Dividimos x^2+1 entre $2x+1$.
Este inverso ya está calculado y vale $\frac{1-2x}{5}$.
Veamos otra forma de haber calculado este inverso.
Notemos que en A, $x^2 = -1$, ya que al dividir x^2 entre x^2+1 el resto es -1.
Escribiremos entonces i en lugar de x (se tiene que $i^2 = -1$).
Calculamos $(1+2i)^{-1} = \frac{1}{1+2i}$.

$$\frac{1}{1+2i} = \frac{1\cdot(1-2i)}{(1+2i)\cdot(1-2i)}$$

Inversos modulares de polinomios. Ejemplo 4.

Vamos a tomar por último $A = \mathbb{R}[x]_{x^2+1}$.
Aquí vamos a calcular $(2x+1)^{-1}$.
Dividimos x^2+1 entre $2x+1$.
Este inverso ya está calculado y vale $\frac{1-2x}{5}$.
Veamos otra forma de haber calculado este inverso.
Notemos que en A, $x^2 = -1$, ya que al dividir x^2 entre x^2+1 el resto es -1.
Escribiremos entonces i en lugar de x (se tiene que $i^2 = -1$).
Calculamos $(1+2i)^{-1} = \frac{1}{1+2i}$.

$$\frac{1}{1+2i} = \frac{1\cdot(1-2i)}{(1+2i)\cdot(1-2i)} = \frac{1-2i}{1^2-(2i)^2}$$

Inversos modulares de polinomios. Ejemplo 4.

Vamos a tomar por último $A = \mathbb{R}[x]_{x^2+1}$.
Aquí vamos a calcular $(2x+1)^{-1}$.
Dividimos x^2+1 entre $2x+1$.
Este inverso ya está calculado y vale $\frac{1-2x}{5}$.
Veamos otra forma de haber calculado este inverso.
Notemos que en A, $x^2 = -1$, ya que al dividir x^2 entre x^2+1 el resto es -1.
Escribiremos entonces i en lugar de x (se tiene que $i^2 = -1$).
Calculamos $(1+2i)^{-1} = \frac{1}{1+2i}$.

$$\frac{1}{1+2i} = \frac{1\cdot(1-2i)}{(1+2i)\cdot(1-2i)} = \frac{1-2i}{1^2-(2i)^2} = \frac{1-2i}{1-4i^2}$$

Inversos modulares de polinomios. Ejemplo 4.

Vamos a tomar por último $A = \mathbb{R}[x]_{x^2+1}$.
Aquí vamos a calcular $(2x+1)^{-1}$.
Dividimos x^2+1 entre $2x+1$.
Este inverso ya está calculado y vale $\frac{1-2x}{5}$.
Veamos otra forma de haber calculado este inverso.
Notemos que en A, $x^2=-1$, ya que al dividir x^2 entre x^2+1 el resto es -1.
Escribiremos entonces i en lugar de x (se tiene que $i^2=-1$).
Calculamos $(1+2i)^{-1} = \frac{1}{1+2i}$.

$$\frac{1}{1+2i} = \frac{1\cdot(1-2i)}{(1+2i)\cdot(1-2i)} = \frac{1-2i}{1^2-(2i)^2} = \frac{1-2i}{1-4i^2} = \frac{1-2i}{1-4(-1)}$$

Vamos a tomar por último $A = \mathbb{R}[x]_{x^2+1}$.
Aquí vamos a calcular $(2x+1)^{-1}$.
Dividimos x^2+1 entre $2x+1$.
Este inverso ya está calculado y vale $\frac{1-2x}{5}$.
Veamos otra forma de haber calculado este inverso.
Notemos que en A, $x^2 = -1$, ya que al dividir x^2 entre x^2+1 el resto es -1.
Escribiremos entonces i en lugar de x (se tiene que $i^2 = -1$).
Calculamos $(1+2i)^{-1} = \frac{1}{1+2i}$.

$$\frac{1}{1+2i} = \frac{1\cdot(1-2i)}{(1+2i)\cdot(1-2i)} = \frac{1-2i}{1^2-(2i)^2} = \frac{1-2i}{1-4i^2} = \frac{1-2i}{1-4(-1)} = \frac{1-2i}{1+4}$$

Inversos modulares de polinomios. Ejemplo 4.

Vamos a tomar por último $A = \mathbb{R}[x]_{x^2+1}$.
Aquí vamos a calcular $(2x+1)^{-1}$.
Dividimos x^2+1 entre $2x+1$.
Este inverso ya está calculado y vale $\frac{1-2x}{5}$.
Veamos otra forma de haber calculado este inverso.
Notemos que en A, $x^2 = -1$, ya que al dividir x^2 entre x^2+1 el resto es -1.
Escribiremos entonces i en lugar de x (se tiene que $i^2 = -1$).
Calculamos $(1+2i)^{-1} = \frac{1}{1+2i}$.

$$\frac{1}{1+2i} = \frac{1\cdot(1-2i)}{(1+2i)\cdot(1-2i)} = \frac{1-2i}{1^2-(2i)^2} = \frac{1-2i}{1-4i^2} = \frac{1-2i}{1-4(-1)} = \frac{1-2i}{1+4} = \frac{1-2i}{5}$$

Inversos modulares de polinomios. Ejemplo 4.

Vamos a tomar por último $A = \mathbb{R}[x]_{x^2+1}$.
Aquí vamos a calcular $(2x+1)^{-1}$.
Dividimos x^2+1 entre $2x+1$.
Este inverso ya está calculado y vale $\frac{1-2x}{5}$.
Veamos otra forma de haber calculado este inverso.
Notemos que en A, $x^2 = -1$, ya que al dividir x^2 entre x^2+1 el resto es -1.
Escribiremos entonces i en lugar de x (se tiene que $i^2 = -1$).
Calculamos $(1+2i)^{-1} = \frac{1}{1+2i}$.

$$\frac{1}{1+2i} = \frac{1\cdot(1-2i)}{(1+2i)\cdot(1-2i)} = \frac{1-2i}{1^2-(2i)^2} = \frac{1-2i}{1-4i^2} = \frac{1-2i}{1-4(-1)} = \frac{1-2i}{1+4} = \frac{1-2i}{5}$$

Como vemos, los resultados coinciden.