# Ejemplos DFU

1. Factorizar $11+7i$ en producto de irreducibles en $\mathbb{Z}[i]$.

$N(11+7i) = 170 = 2 \cdot 5 \cdot 17$

$\boxed{N(\alpha)=2}$

$1+i \quad -1-i \quad -1+i \quad 1-i$

$$\frac{11+7i}{1+i} = \frac{(11+7i)(1-i)}{2} = \frac{11-11i+7i+7}{2} = 9-2i$$

$\boxed{N(\beta)=5}$

$1+2i \quad -1-2i \quad -2+i \quad 2-i$ } Asociados

$1-2i \quad -1+2i \quad 2+i \quad -2-i$ } Asociados

$$\frac{9-2i}{1+2i} = \frac{(9-2i)(1-2i)}{5} = \frac{9-18i-2i-4}{5} = 1-4i$$

$\boxed{N(\gamma)=17} \Rightarrow$ Ya lo tenemos: $1-4i$

$$11+7i = (1+i)(1+2i)(1-4i)$$

2. Calcular $(2i, 11+7i)$ y $[2i, 11+7i]$ en $\mathbb{Z}[i]$.

$2i \sim 2 \Rightarrow (2i, 11+7i) = (2, 11+7i)$

Por el ejercicio anterior, $11+7i = (1+i)(1+2i)(1-4i)$

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

$(2i, 11+7i) = 1+i$

$[2i, 11+7i] = (1+i)^2(1+2i)(1-4i) = 2i \cdot (9-2i) = 4+18i$

3. Factorizar $180$ en producto de irreducibles en el anillo $\mathbb{Z}[\sqrt{-2}]$.

$180 = 2^2 \cdot 3^2 \cdot 5$

$N(a+b\sqrt{-2}) = (a+b\sqrt{-2})(a-b\sqrt{-2}) = a^2+2b^2$

¿Es $2$ irreducible en $\mathbb{Z}[\sqrt{-2}]$?

$N(2)=4$ ¿$\exists \alpha$ tq $N(\alpha)=2$? $\Rightarrow a^2+2b^2=2$ Sí, cuando $a=0$ y $b=\pm 1$

$\boxed{N(\alpha)=2} \Rightarrow \sqrt{2}$ y $\sqrt{-2}$

$$\frac{2}{\sqrt{2}} = \frac{2\sqrt{2}}{2} = \sqrt{2} \Rightarrow 2 = -(\sqrt{-2})^2$$

¿Es 3 irreducible?

$N(3)=9$ ¿$\exists \alpha \in \mathbb{Z}[\sqrt{-2}]$ tq $N(\alpha)=3$?

$a^2+2b^2=3 \Rightarrow$ Sí, cuando $a=\pm 1$ y $b=\pm 1$

Es decir, $1+\sqrt{-2}, 1-\sqrt{-2}, -1+\sqrt{-2}, -1-\sqrt{-2}$:

$$\frac{3}{1+\sqrt{-2}} = \frac{3(1-\sqrt{-2})}{3} = 1-\sqrt{-2} \Rightarrow 3 = (1+\sqrt{-2})(1-\sqrt{-2})$$

¿Es 5 irreducible?

$N(5)=25$ ¿$\exists \alpha \in \mathbb{Z}[\sqrt{-2}]$ tq $N(\alpha)=5$?

$a^2+2b^2=5 \Rightarrow$ No tiene solución

Factorización buscada:

$$180 = (\sqrt{-2})^4(1+\sqrt{-2})^2(1-\sqrt{-2})^2 \cdot 5$$

4. En $\mathbb{Z}[\sqrt{-5}]$ hay irreducibles que no son primos.

Irreducible: No tiene divisores propios.
Primo: Si $p|ab$, entonces $p|a$ ó $p|b$.

$$N(a+b\sqrt{-5}) = (a+b\sqrt{-5})(a-b\sqrt{-5}) = a^2+5b^2$$

Ej.:
$1+\sqrt{-5}$ es irreducible ya que no existen elementos en $\mathbb{Z}[\sqrt{-5}]$ de norma 2 y 3, y $N(1+\sqrt{-5})=6=2\cdot 3$.
$1-\sqrt{-5}$ lo es por la misma razón, al igual que 2 y 3.

Además, 2 no es primo, pues $2|6=(1+\sqrt{-5})(1-\sqrt{-5})$ pero $2\nmid(1+\sqrt{-5})$ ni tampoco $2\nmid(1-\sqrt{-5})$.

5. Factoriza $f = x^5 + x^4 + 1$ en $\mathbb{Z}_2[x]$.

$f(0) = 1 \quad f(1) = 1 \Rightarrow$ No tiene raíces $\Rightarrow$ Tampoco tendrá factores de grado 4. Veamos si es divisible por $x^2+x+1$:

$$\begin{array}{l|l} x^5+x^4+1 & x^2+x+1 \\ \hline +x^5+x^4+x^3 & x^3+x+1 \\ \hline x^3+1 & \\ +x^3+x^2+x & \\ \hline x^2+x+1 & \\ +x^2+x+1 & \\ \hline 0 & \end{array}$$

Fact. irred.: $x^5+x^4+1 = (x^2+x+1)(x^3+x+1)$

6. Factoriza $f = x^5 + x^4 + x^2 + 1$ en $\mathbb{Z}_3[x]$.

$f(0) = 1 \quad f(1) = 1 \quad f(2) = 2 \Rightarrow$ No tiene raíces $\Rightarrow$ Tampoco tiene factores de grado 4.

$$\begin{array}{l|l} x^5+x^4+x^2+1 & x^2+1 \\ \hline 2x^5+2x^3 & x^3+x^2+2x \\ \hline x^4+2x^3+x^2+1 & \\ 2x^4 \qquad +2x^2 & \\ \hline 2x^3+1 & \\ +x^3+x & \\ \hline x+1 & \end{array}$$

No divide

$$\begin{array}{l|l} x^5+x^4+x^2+1 & x^2+x+2 \\ \hline 2x^5+2x^4+x^3 & x^3+x \\ \hline x^3+x^2+1 & \\ 2x^3+2x^2+x & \\ \hline x+1 & \end{array}$$

No divide

Es irreducible

$$\begin{array}{l|l} x^5+x^4+x^2+1 & x^2+2x+2 \\ \hline 2x^5+x^4+x^3 & x^3+2x^2 \\ \hline 2x^4+x^3+x^2+1 & \\ +x^4+2x^3+2x^2 & \\ \hline 1 & \end{array}$$

No divide

7. Factoriza $f = 20x^4 - 10x^3 - 80x^2 + 80x - 20$ en $\mathbb{Z}[x]$.

$10(2x^4 - x^3 - 8x^2 + 8x - 2)$ $\quad a \mid a_0 \Rightarrow a = \pm 1, \pm 2$

$b \mid a_n \Rightarrow b = \pm 1, \pm 2$

$f\left(\frac{a}{b}\right) \quad \frac{a}{b} \left\{ \pm 1, \pm \frac{1}{2}, \pm 2 \right. \Rightarrow$ Posibles raíces

$f(-1) \neq 0 \quad f(1) \neq 0 \quad f(2) \neq 0 \quad f(-2) \neq 0 \quad f\left(-\frac{1}{2}\right) \neq 0 \quad f\left(\frac{1}{2}\right) = 0$

$$
\begin{array}{l|l}
2x^4 - x^3 - 8x^2 + 8x - 2 & 2x-1 \\ \cline{2-2}
-2x^4 + x^3 & x^3 - 4x + 2 \\ \hline
\qquad -8x^2 + 8x - 2 & \\
\qquad +8x^2 - 4x & \\ \hline
\qquad\qquad 4x - 2 & \\
\qquad\quad -4x + 2 & \\ \hline
\qquad\qquad\quad 0 &
\end{array}
$$

$x^3-4x+2$ es irred. pues las únicas posibles raíces son: $a \mid a_0$ $\quad b \mid a_n$

$$\Downarrow \qquad\qquad \Downarrow$$

$$a = \pm 1, \pm 2 \qquad b = \pm 1 \Rightarrow \frac{a}{b} \left\{ \pm 1, \pm 2 \right.$$

Pero ya hemos visto que no son raíces, por lo que $x^3-4x+2$ es irreducible y tenemos que:

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

7. Factoriza $f = x^3 + \frac{1}{2}x^2 - x + 3$ en $\mathbb{Q}[x]$.

$$f = \frac{1}{2}(\underbrace{2x^3 + x^2 - 2x + 6}_{\text{Lo estudiamos en } \mathbb{Z}[x]})$$

$$\left.\begin{array}{l} a \mid a_0 \Rightarrow a = \pm 1, \pm 2, \pm 3, \pm 6 \\ b \mid a_n \Rightarrow b = \pm 1, \pm 2 \end{array}\right\} \frac{a}{b} \left\{ \pm 1, \pm 2, \pm 3, \pm 6, \pm \frac{3}{2}, \pm \frac{1}{2} \right.$$

$$f\left(\frac{3}{2}\right) = 0 \Rightarrow
\begin{array}{l|l}
2x^3 + x^2 - 2x + 6 & 2x-3 \\ \cline{2-2}
-2x^3 + 3x^2 & x^2 + 2x + 2 \\ \hline
\qquad 4x^2 - 2x + 6 & \\
\quad -4x^2 + 6x & \\ \hline
\qquad\qquad 4x + 6 &
\end{array}
$$

En $\mathbb{Z}[\sqrt{-2}]$ encuentra el inverso de $1+3\sqrt{-2}$ modulo $3+5\sqrt{-2}$.

$$N(1+3\sqrt{-2}) = (1+3\sqrt{-2})(1-3\sqrt{-2}) = 1-3\sqrt{-2}+3\sqrt{-2}+18 = 19$$

$$N(3+5\sqrt{-2}) = (3+5\sqrt{-2})(3-5\sqrt{-2}) = 9-15\sqrt{-2}+15\sqrt{-2}+50 = 59$$

$$\frac{3+5\sqrt{-2}}{1+3\sqrt{-2}} = \frac{(3+5\sqrt{-2})(1-3\sqrt{-2})}{19} = \frac{3-4\sqrt{-2}+30}{19} \simeq 2$$

$(3+5\sqrt{-2}) = (1+3\sqrt{-2})2 + R \Rightarrow$ Resto $= 1-\sqrt{-2}$

$$\frac{1+3\sqrt{-2}}{1-\sqrt{-2}} = \frac{(1+3\sqrt{-2})(1+\sqrt{-2})}{3} = \frac{1+4\sqrt{-2}-6}{3} = -2+\sqrt{-2}$$

$(1-\sqrt{-2})(-2+\sqrt{-2}) = -2+3\sqrt{-2}+2 = 3\sqrt{-2} \Rightarrow$ Resto $= 1$

| | | | |
|---|---|---|---|
| | $3+5\sqrt{-2}$ | $1$ | $0$ |
| | $1+3\sqrt{-2}$ | $0$ | $1$ |
| $2$ | $1-\sqrt{-2}$ | $1$ | $-2$ |
| $-2+\sqrt{-2}$ | $1$ | $2-\sqrt{-2}$ | $-3+2\sqrt{-2}$ |

$$(3+5\sqrt{-2})(2-\sqrt{-2}) + (1+3\sqrt{-2})(-3+2\sqrt{-2}) = 1$$

El inverso de $1+3\sqrt{-2}$ mod$(3+5\sqrt{-2})$ es $-3+2\sqrt{-2}$

En $\mathbb{Z}[i]$ factoriza como producto de irreducibles $-11+7i$.

$$N(-11+7i) = 170 = 2\cdot 5\cdot 17$$

Buscamos el divisor de norma 2:

Norma 2: $1+i, -1-i, -1+i, 1-i$

$$\frac{-11+7i}{1+i} = \frac{(-11+7i)(1-i)}{2} = \frac{-11+11i+7i+7}{2} = -2+9i$$

Buscamos el divisor de norma 5:

Norma 5: $1+2i, -1-2i, -2+i, 2-i$ } Asociados

$1-2i, -1+2i, 2+i, -2-i$ } Asociados

$$\frac{-2+9i}{2+i} = \frac{(-2+9i)(2-i)}{5} = \frac{-4+2i+18i+9}{5} = 1+4i \Rightarrow$$ Este es irreducible de norma 17.

Fact.: $-11+7i = (1+i)(2+i)(1+4i)$

Factoriza el polinomio $x^4+7x^3+x^2+2x+1$ en $\mathbb{Z}[x]$.

$a \mid a_0 \Rightarrow a = \pm 1$ Posibles raíces: $\pm 1$

$b \mid a_n \Rightarrow b = \pm 1$

$f(-1) = -6 \neq 0 \Rightarrow$ No tiene factores lineales por lo que tampoco tendrá de grado 3.

Módulo 2

$$\begin{array}{l|l} x^4+x^3+x^2+1 & x^2+x+1 \\ \hline x^4+x^3+x^2 & x^2 \\ \hline \quad\quad 1 & \end{array}$$

$\Rightarrow$ No tiene factores de grado 2 ni 3 en $\mathbb{Z}_2[x]$, por lo que tampoco en $\mathbb{Z}[x]$.

$x^4+7x^3+x^2+2x+1$ es irreducible en $\mathbb{Z}[x]$.

Resuelve la siguiente ecuación en $\mathbb{Z}_3[x]$:

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

y encuentra una solución en la que el grado del polinomio $F(x)$ sea mínimo.

$$\begin{array}{l|l} x^4+2x^3+x^2+2 & x^3+2x^2+x+2 \\ \hline 2x^4+x^3+2x^2+x & x \\ \hline \quad\quad x+2 & \end{array} \qquad \begin{array}{l|l} x^3+2x^2+x+2 & x+2 \\ \hline 2x^3+x^2 & x^2+1 \\ \hline \quad x+2 & \\ \quad 2x+1 & \\ \hline \quad\quad 0 & \end{array}$$

$$\begin{array}{c|c|cc} & x^4+2x^3+x^2+2 & 1 & 0 \\ & x^3+2x^2+x+2 & 0 & 1 \\ x & x+2 & 1 & 2x \end{array}$$

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

$$\begin{array}{l|l} x^2+2 & x+2 \\ \hline 2x^2+x & x+1 \\ \hline \quad x+2 & \\ \quad 2x+1 & \\ \hline \quad\quad 0 & \end{array}$$

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

Sol.: $\begin{cases} F(x) = 2x^2+2x + k(x^3+x+1) \\ G(x) = x+1 + k(2x^2+2) \end{cases}$

$$\begin{array}{l|l} x^4-x^3+x^2-1 & x+2 \\ \hline 2x^4+x^3 & x^3+x+1 \\ \hline \quad x^2-1 & \\ \quad 2x^2+x & \\ \hline \quad\quad x-1 & \end{array}$$

$F(x)$ mínimo: $2x^2+2x$