Examen Álgebra I, Doble Grado Informática Matemáticas, Enero 2020

Nombre::____

1. El banco CCC utiliza para codificar el número secreto de sus usuarios el método RSA con llaves públicas $e = 107$ y $n = 5616$. Al codificar el número secreto de Antonio obtenemos 4903, calcula el número secreto de Antonio.

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

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

4. En el anillo $\mathbb{Z}[\sqrt{2}]$ considera los ideales $I =< 12+7\sqrt(2) >, J =< 8+5\sqrt(2) >$. ¿Es el ideal $I \cap J$ principal? En caso afirmativo encuentra un generador.

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

6. Encuentra un cuerpo de característica 2 con 4 elementos. Razona la respuesta.

7. Del polinomio $f(x) = x^6 + 10x^4 + 2x^3 + 21x^2 + 10x + 1$ sabemos que tienen un factor g que cumple:

- $g(0) = 1$,
- $g(1) = 5$ y
- el resto de dividir g por $x^2 + x + 1$ es $3x + 2$.

Factoriza $f(x)$ como producto de polinomios irreducibles.

Ejercicio Ordinaria

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

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

$N(3+5\sqrt{-2}) = 3^2 + 2\cdot 5^2 = 59$

$$\frac{3+5\sqrt{-2}}{1+3\sqrt{-2}} = \frac{(3+5\sqrt{-2})(1-3\sqrt{-2})}{19} = \frac{33-4\sqrt{-2}}{19} \simeq 2$$

Resto $= 1-\sqrt{-2}$

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

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

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

$1+2(-2+\sqrt{-2})$

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

Ejercicio Ordinaria

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

- No nos sirve Eisenstein.
- $a \mid a_0 \Rightarrow a_0 = \pm 1$, $b \mid a_n \Rightarrow b_0 = \pm 1$ $\Big\}$ Posibles raíces: $\pm 1 \Rightarrow$ Ninguna lo anula, no tiene factores lineales por lo que tampoco de grado 3.

Pasamos a módulo 2:

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

$f(1)=0 \Rightarrow$ Tiene factores lineales

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

$\Rightarrow x^4+x^3+x^2+1 = (x+1)\underbrace{(x^3+x+1)}_{\text{No tiene factores lineales,}}$

por lo que tampoco de grado 2 y concluimos que $x^4+7x^3+x^2+2x+1$ tampoco los tiene y es irreducible

Ejercicio Ordinaria

$f(x) = x^6 + 10x^4 + 2x^3 + 21x^2 + 10x + 1$

$$\begin{cases} g(x) \equiv 1 \pmod{x} \\ g(x) \equiv 5 \pmod{x-1} \\ g(x) \equiv 3x+2 \pmod{x^2+x+1} \end{cases}$$

$g(x) = (3x+2) + (x^2+x+1)t$

$(3x+2) + (x^2+x+1)t \equiv 5 \pmod{x-1}$

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

$5 + 3t \equiv 5 \pmod{x-1}$

$3t \equiv 0 \pmod{x-1}$

$t \equiv 0 \pmod{x-1}$

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

$(3x+2) + (x^3-1)s \equiv 1 \pmod{x}$

$2 + (x^3-1)s \equiv 1 \pmod{x}$

$2 - s \equiv 1 \pmod{x}$

$s \equiv 1 \pmod{x}$

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

$$\boxed{\text{Sol.: } (3x+2) + (x^3-1)(1+xk) = x^3+3x+1 + (x^4-x)k}$$

$= x^3+3x+1$

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

$$\begin{array}{l|l} x^6+10x^4+2x^3+21x^2+10x+1 & x^3+3x+1 \\ \hline -x^6-3x^4-x^3 & x^3+7x+1 \\ \hline 7x^4+x^3+21x^2+10x+1 & \\ -7x^4 \quad -21x^2-7x & \\ \hline x^3 \quad +3x+1 & \\ -x^3 \quad -3x-1 & \\ \hline 0 & \end{array}$$

$(x^3+3x+1)(x^3+7x+1)$

Veamos si son irreducibles

$\boxed{x^3+3x+1} \Rightarrow$ Posibles raíces: $\pm 1 \Rightarrow$ No la anulan

$\boxed{x^3+7x+1} \Rightarrow$ Posibles raíces: $\pm 1 \Rightarrow$ No la anulan

Son irred.

$$\boxed{x^6+10x^4+2x^3+21x^2+10x+1 = (x^3+3x+1)(x^3+7x+1)}$$

Ejercicio Ordinaria

En $\mathbb{Z}[\sqrt{2}]$, $I = \langle 12 + 7\sqrt{2} \rangle$, $J = \langle 8 + 5\sqrt{2} \rangle$. ¿Es $I \cap J$ un ideal principal? Si lo es, encuentra un generador.

Sí lo es, ya que en teoría, sabemos quen en los DE, $aA \cap bA = [a,b]A$. Por ello, hemos de hallar el m.c.m $(12+7\sqrt{2}, 8+5\sqrt{2})$, que será el generador de $I \cap J$:

$$N(a+b\sqrt{2}) = (a+b\sqrt{2})(a-b\sqrt{2}) = a^2 - 2b^2$$
$$N(12+7\sqrt{2}) = 46 \quad N(8+5\sqrt{2}) = 14$$

$$\frac{12+7\sqrt{2}}{8+5\sqrt{2}} = \frac{(12+7\sqrt{2})(8-5\sqrt{2})}{14} = \frac{26-4\sqrt{2}}{14} \simeq 2$$

Resto $= -4-3\sqrt{2}$

$$\frac{8+5\sqrt{2}}{-4-3\sqrt{2}} = \frac{(8+5\sqrt{2})(-4+3\sqrt{2})}{-2} = 1-2\sqrt{2} \quad \text{Resto} = 0$$

Por lo tanto, m.c.d. $(12+7\sqrt{2}, 8+5\sqrt{2}) = -4-3\sqrt{2}$

$$\text{m.c.m.}(12+7\sqrt{2}, 8+5\sqrt{2}) = \frac{(12+7\sqrt{2})(8+5\sqrt{2})}{-4-3\sqrt{2}} =$$

$$= \frac{96+70+116\sqrt{2}}{-4-3\sqrt{2}} = \frac{(166+116\sqrt{2})(-4+3\sqrt{2})}{(-4-3\sqrt{2})(-4+3\sqrt{2})} = \frac{32+34\sqrt{2}}{-2} =$$

$$= -16-17\sqrt{2}$$