Examen Final Álgebra I

Alumno: José Alberto Hoces Castro

Este fue el único que no hice porque me equivoqué con las cuentas, en el resto tuve puntuación perfecta

1. Factorizar $x^6-3x^4+6x^2+6x+1$ en $\mathbb{Z}[x]$

2. Factorizar en $\mathbb{Z}[i]$ el elemento $\alpha = 7-6i$

Primero veamos su norma: $N(7-6i) = 85 = 5 \cdot 17$

En vista de su norma, se deduce que $7-6i$ se puede descomponer como el producto de dos irreducibles de norma 5 y de norma 17. Veamos cuáles dividen a $7-6i$:

ELEMENTOS DE NORMA 5

$$2+i \sim -2-i \sim -1+2i \sim 1-2i$$

$$2-i \sim -2+i \sim 1+2i \sim -1-2i$$

$$\frac{7-6i}{2+i} = \frac{(7-6i)(2-i)}{5} = \frac{8-19i}{5} \Rightarrow \text{No divide}$$

$$\frac{7-6i}{2-i} = \frac{(7-6i)(2+i)}{5} = 4-i$$

$N(4-i) = 17 \Rightarrow$ Es un irreducible de norma 17

Por lo tanto, $\boxed{\alpha = 7-6i = (2-i)(4-i)}$

Alumno: José Alberto Hoces Castro

3.

$$\begin{cases} 2x \equiv 138 \pmod{153} \\ 3x \equiv 1 \pmod{95} \end{cases}$$

Primero he de simplificar el sistema.

$153 \,\underline{|2}$; $1 \quad 76$

$$\begin{array}{c|c|cc} & 153 & 1 & 0 \\ & 2 & 0 & 1 \\ 76 & 1 & 1 & -76 \end{array} \Rightarrow 153 \cdot 1 + 2 \cdot (-76) = 1$$

$$2x \equiv 138 \pmod{153} \Rightarrow x \equiv 69 \pmod{153}$$

$95 \,\underline{|3}$; $2 \quad 31$ $\qquad$ $3 \,\underline{|2}$; $1 \quad 1$

$$\begin{array}{c|c|cc} & 95 & 1 & 0 \\ & 3 & 0 & 1 \\ 31 & 2 & 1 & -31 \\ 1 & 1 & -1 & 32 \end{array}$$

$95(-1) + 3 \cdot 32 = 1$

$$x \equiv 32 \pmod{95}$$

$$\begin{cases} x \equiv 69 \pmod{153} \Rightarrow x = 69 + 153t \\ x \equiv 32 \pmod{95} \end{cases}$$

sustituimos

$$69 + 153t \equiv 32 \pmod{95}$$
$$58t \equiv -37 \pmod{95}$$
$$58t \equiv 58 \pmod{95}$$

Como $58 = 2 \cdot 29$ y $95 = 5 \cdot 19$, son primos relativos y existe el inverso de 58 (mod 95), no hace falta buscarlo, y tenemos que:

$$t \equiv 1 \pmod{95}$$
$$t = 1 + 95k$$

Y sustituimos en x:

$$x = 69 + 153t = 69 + 153(1 + 95k) = 222 + 14535k$$

$$\boxed{\text{Sol.: } 222 + 14535k \text{ con } k \in \mathbb{Z}}$$

Un número mayor que 14535 que cumpla dicho sistema se obtiene sustituyendo en la solución general $k = 1$: $\boxed{14757}$ ⟸ Este es el número que me pedían

Alumno: José Alberto Hoces Castro

4. $f: \mathbb{Z}_{10} \to \mathbb{Z}_{10}$; $f(x) := x^4 \pmod{10}$; R_f

¿f inyectiva, sobreyectiva o biyectiva?

$f(0)=0$	$f(5)=5$
$f(1)=1$	$f(6)=6$
$f(2)=6$	$f(7)=1$
$f(3)=1$	$f(8)=6$
$f(4)=6$	$f(9)=1$

No es inyectiva ya que hay elementos del dominio con la misma imagen como 2, 4, 6 y 8, que tienen de imagen al 6. Tampoco es sobreyectiva ya que hay elementos de $\mathbb{Z}_{10}$ que no son imagen de ningún elemento de $\mathbb{Z}_{10}$, como por ejemplo 2, 3, 4, 7, 8 y 9.

Conjunto cociente $\mathbb{Z}_{10}/R_f$

Dos elementos serán de la misma clase si tienen misma imagen, por lo que habrá tantas clases como imágenes (voy a nombrar cada clase por la imagen que la representa, es decir, la clase de los elementos cuya imagen sea 6 la escribiré como [6], y así con todos):

$$\mathbb{Z}_{10}/R_f = \{[0],[1],[5],[6]\}$$

- $[0]$: 1 representante $\boxed{0}$
- $[1]$: 4 representantes $\boxed{1,3,7,9}$
- $[5]$: 1 representante $\boxed{5}$
- $[6]$: 4 representantes $\boxed{2,4,6,8}$

¿Puedo definir $g: \mathbb{Z}_{10}/R_f \to \mathbb{Z}_{10}$ por la fórmula $g(\bar{x}) := x^2 \pmod{10}$?

No se puede ya que cada clase tendría varias imágenes y no estaría bien definida. Esto se debe a que la imagen de la clase dependería del representante que se coja. Por ejemplo:

$$\left.\begin{array}{l} g([1]) = 3^2 \pmod{10} = 9 \pmod{10} \\ g([1]) = 9^2 \pmod{10} = 1 \pmod{10} \end{array}\right\} \Rightarrow \text{No está bien definida}$$

"3 y 9 son de la misma clase"

Alumno: José Alberto Hoces Castro

5. Calcular $\varphi(120)$ y $19^{-1234567} \pmod{120}$

$120 = 2^3 \cdot 3 \cdot 5$

$\varphi(120) = 120\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right) = 32$

Como m.c.d.$(120, 19) = 1$, podemos aplicar el teorema de Fermat: $19^{32} \equiv 1 \pmod{120}$

$-1234567 \pmod{32}$

Puedo sumar $32 \cdot 40000$ a -1234567 y tengo que: $45433 \pmod{32}$

(No varía nada pues sumar $32 \cdot 40000$ es como sumar 0 módulo 32, pero nos facilita las cosas)

$45433 \pmod{32} = 25 \pmod{32}$

Por lo tanto:

$19^{-1234567} \pmod{120} = 19^{25} \pmod{120}$

$19^5 \pmod{120} = 19 \pmod{120}$

$[19^5]^5 \pmod{120} = [19]^5 \pmod{120} = 19 \pmod{120}$

Resultados: $\boxed{\varphi(120) = 32}$, $\boxed{19 \pmod{120}}$

Alumno: José Alberto Hoces Castro