Muy buen parcial

1	2	3	4	5		Calif.
B	B	B	B	B		A

Apellido y Nombre:
Turno: ~~☐~~ Mañana (8-

Álgebra I - 2do Cuatrimestre 2016

Segundo Recuperatorio del Segundo Parcial - 16/12/2016

---

1. Determinar todos los $a \in \mathbb{N}$ para los cuales $\dfrac{a^{255}-1}{45}$ es un número entero.

2. Determinar todos los $n \in \mathbb{N}$ tales que $3^{108n+15} \equiv 5n (19)$.

3. Sea $z \in G_{256}$. Determinar los posibles valores de

$$(z^2-1)\sum_{i=0}^{63} z^{2i}.$$

4. Sean $f(X) = X^5 - 2X^4 + 3X^2 - 4X + 2$, $g(X) = X^4 - X^3 + 3X^2 - 2X + 2$. Factorizar f en $\mathbb{Q}[X]$, $\mathbb{R}[X]$ y $\mathbb{C}[X]$ sabiendo que f y g tienen raíces comunes.

5. Probar que $X^{2016} + 2X^{1833} - X^{174} + X^{137} + 2X^4 - X^3 + 1$ es divisible por $X^4 + X^3 + X^2 + X + 1$.

Complete esta hoja con sus datos y entréguela con el resto del examen.
Justifique todas sus respuestas.

Ejercicio 4

$f(x) = x^5 - 2x^4 + 3x^2 - 4x + 2$ y $g(x) = x^4 - x^3 + 3x^2 - 2x + 2$

f y g tienen raíces comunes, por lo tanto hay por lo menos un factor $x - \alpha$ tal que $x - \alpha \mid f$ y $x - \alpha \mid g$ porque α es raíz común de g y f. Por lo tanto, como $x - \alpha \mid f$ y $x - \alpha \mid g \Rightarrow x - \alpha \mid (f:g) \Rightarrow$ $(f:g) \neq 1$.

Las raíces de $(f:g)$ son las raíces que tienen en común f y g. ($(f:g) \mid f$ y $(f:g) \mid g$)

Voy a calcular $(f:g)$ mediante el algoritmo de Euclides

$$\begin{array}{rl}
x^5 - 2x^4 + 3x^2 - 4x + 2 & \underline{\mid x^4 - x^3 + 3x^2 - 2x + 2} \\
\ominus\ \underline{x^5 - x^4 + 3x^3 - 2x^2 + 2x} & x - 1 \\
-x^4 - 3x^3 + 5x^2 - 6x + 2 & \\
\ominus\ \underline{-x^4 + x^3 - 3x^2 + 2x - 2} & \\
-4x^3 + 8x^2 - 8x + 4 &
\end{array}$$

$-4x^3 + 8x^2 - 8x + 4 = -4(x^3 - 2x^2 + 2x - 1)$ (lo hice mónico)

$$\begin{array}{rl}
x^4 - x^3 + 3x^2 - 2x + 2 & \underline{\mid x^3 - 2x^2 + 2x - 1} \\
\ominus\ \underline{x^4 - 2x^3 + 2x^2 - x} & x + 1 \\
x^3 + x^2 - x + 2 & \\
\ominus\ \underline{x^3 - 2x^2 + 2x - 1} & \\
3x^2 - 3x + 3 &
\end{array}$$

$\rightarrow 3x^2 - 3x + 3 = 3(x^2 - x + 1)$ (lo hice mónico)

$$\begin{array}{rl}
x^3 - 2x^2 + 2x - 1 & \underline{\mid x^2 - x + 1} \\
\ominus\ \underline{x^3 - x^2 + x} & x - 1 \\
-x^2 + x - 1 & \\
\ominus\ \underline{-x^2 + x - 1} & \\
0 &
\end{array}$$

$\rightarrow$ como el resto dio 0, el MCD es el resto anterior (último resto no nulo).

$(f:g) = x^2 - x + 1$.

$(f:g) = x^2 - x + 1 \Rightarrow f = (x^2-x+1)\, q$

busco ese q dividiendo a f por el mcD

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

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

ninguno de estos factores es irreducible en $\mathbb{C}$ → (grado $\neq 1$)

x^3-x^2-2x+2 → podemos tratar de encontrar sus raices con gauss.

Si tiene raices racionales, estas son algunos de los siguientes candidatos: $\alpha = \frac{\text{div}(2)}{\text{div}(1)} \to 2, -2, 1, -1$

$\Rightarrow f(2) \neq 0 \quad \boxed{f(1) = 0} \quad f(-2) \neq 0 \quad f(-1) \neq 0$

como 1 es raiz, $x-1 \mid x^3-x^2-2x+2$

$$\begin{array}{l|l} x^3-x^2-2x+2 & x-1 \\ \ominus\ x^3-x^2 & \overline{x^2-2} \\ \hline -2x+2 & \\ \ominus\ -2x+2 & \\ \hline 0 & \end{array}$$

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

x^2-2 tiene raices en $\mathbb{R}$

→ $x^2-2=0$

$x^2 = 2$

$x = \sqrt{2} \qquad x = -\sqrt{2}$

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

$\Rightarrow f = (x-1)(x-\sqrt{2})(x+\sqrt{2})(x^2-x+1)$

Asamblea

Ahora busco las raices de $x^2 - x + 1$

$x^2 - x + 1 = 0$

~~en~~ $\frac{1 \pm w}{2}$ con $w /$ $w^2 = 1 - 4 = -3$

$w^2 = -3$

$w_1 = \sqrt{3}\, i$ $\quad w_2 = -\sqrt{3}\, i$

entonces los x que cumplen $x^2 - x + 1 = 0$ son:

$\frac{1 \pm \sqrt{3}\, i}{2} = \frac{1}{2} \pm \frac{\sqrt{3}}{2} i$ $\quad \frac{1}{2} + \frac{\sqrt{3}}{2} i$, $\quad \frac{1}{2} - \frac{\sqrt{3}}{2} i$ efectivamente $f(z) = 0 \Leftrightarrow f(\bar{z}) = 0$.

$x^2 - x + 1 = \left(x - \left(\frac{1}{2} - \frac{\sqrt{3}}{2} i\right)\right)\left(x - \left(\frac{1}{2} + \frac{\sqrt{3}}{2} i\right)\right)$.

en $\mathbb{C}[x]$

$\Rightarrow f = (x-1)(x-\sqrt{2})(x+\sqrt{2})\left(x - \left(\frac{1}{2} + \frac{\sqrt{3}}{2} i\right)\right)\left(x - \left(\frac{1}{2} - \frac{\sqrt{3}}{2} i\right)\right)$

↳ esta es la factorización en $\mathbb{C}[x]$ $\Rightarrow$ son todos ~~termin~~ factores de grado 1 $\Rightarrow$ irreducibles en $\mathbb{C}[x]$.

en $\mathbb{R}[x]$

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

Los primeros 3 factores son irreducibles por ser de grado 1

el último factor es irreducible por ser de grado 2 y por no tener raíces reales. $\left(\frac{1}{2} - \frac{\sqrt{3}}{2} i \text{ y } \frac{1}{2} + \frac{\sqrt{3}}{2} i \notin \mathbb{R}\right)$.

en $\mathbb{Q}[x]$

$f = (x-1)(x^2-2)(x^2-x+1)$.

$(x-1)$: gr $= 1$ (irreducible)

$x^2 - 2$ es irreducible en $\mathbb{Q}[x]$ porque es de grado $= 2$ y no tiene raices racionales $(\sqrt{2}$ y $-\sqrt{2} \notin \mathbb{Q})$.

$x^2 - x + 1$ ~~no tiene~~ es irreducible en $\mathbb{Q}[x]$ porque tiene grado 2 y no tiene raices racionales.

Ejercicio 3

$z \in G_{256}$. $\quad 256 = 2^8$

~~Sé que~~

$$(z^2-1)\cdot\sum_{i=0}^{63}(z^2)^i = \cancel{(z^2-1)}\,\frac{(z^2)^{63+1}-1}{\cancel{(z^2-1)}} \quad (\text{Si } z^2-1\neq 0)$$

$$= z^{128}-1$$

También sé que:

$$G_{256} = G_2^* \oplus G_4^* \oplus G_8^* \oplus G_{16}^* \oplus G_{32}^* \oplus G_{64}^* \oplus G_{128}^* \oplus G_{256}^* \oplus G_1^* \quad (z \in G_k \text{ primitivas} / k \mid 256)$$

Si $z \in G_{256} \Rightarrow$ ~~[illegible]~~

z es primitiva de G_k. $(k \mid 256)$.

Si $z \in G_1^* \Rightarrow z = 1$.

$\hookrightarrow$ $z^{128}-1 = 1-1 = 0$.

Si $z \in G_2^* \Rightarrow z^2 = 1$ $\Big\}$ $(z^2-1)\sum_{i=0}^{63}(z^2)^i = (1-1)\sum_{i=0}^{63} 1^i = 0$

Si $z \in G_4^* \Rightarrow z^4 = 1$

$\Rightarrow z^{128}-1 = (z^4)^{32}-1 = 1^{32}-1 = 0$.

Si $z \in G_8^* \Rightarrow z^8 = 1 \Rightarrow z^{128}-1 = (z^8)^{16}-1 = 1-1 = 0$.

Si $z \in G_{16}^* \Rightarrow z^{16} = 1 \Rightarrow z^{128}-1 = (z^{16})^8-1 = 1-1 = 0$.

Si $z \in G_{32}^* \Rightarrow z^{32} = 1 \Rightarrow z^{128}-1 = (z^{32})^4-1 = 1-1 = 0$.

Si $z \in G_{64}^* \Rightarrow z^{64} = 1 \Rightarrow z^{128}-1 = (z^{64})^2-1 = 1-1 = 0$.

Si $z \in G_{128}^* \Rightarrow$ ~~z^{128}~~ $z^{128} = 1 \Rightarrow z^{128}-1 = 0$

Si $z \in G_{256}^* \Rightarrow z^{256} = 1 \Rightarrow (z^{128})^2 = 1$.

~~como~~ $w^2 = 1$ $\begin{cases} w=1 \\ w=-1 \end{cases}$ $\Rightarrow z^{128} = 1$ ó $z^{128} = -1$.

pero $z^0 = 1$ ~~[illegible]~~ y $z^k = z^m \Leftrightarrow k = m$

$\Rightarrow z^{128} = -1 \Rightarrow z^{128}-1 = -1-1 = -2$

$\longrightarrow$

Asamblea

En conclusión si $\boxed{z \in G_{256} \text{ es primitivo}} \Rightarrow$

$$(z^2-1)\sum_{i=0}^{63} z^{2i} = \boxed{-2}.$$

si $\boxed{z \in G_{256} \text{ no es primitivo}} \Rightarrow (z^2-1)\sum_{i=0}^{63} z^{2i} = \boxed{0}.$

— o —

Ejercicio 1

$\frac{a^{255}-1}{45}$ es un entero sii $a^{255}-1 \equiv 0 \ (45)$

porque $a^{255}-1$ es un entero porque es una suma de enteros y 45 es un entero $\Rightarrow$

$\frac{a^{255}-1}{45}$ no es entero sii $45 \nmid a^{255}-1$.

busco los $a \in \mathbb{N}$ para los cuales

$$a^{255}-1 \equiv 0 \ (45). \quad 45 = 3^2 \cdot 5.$$

voy a separar la congruencia ~~fact~~ en los factores de 45

$$a^{255}-1 \equiv 0 \ (45) \Leftrightarrow \underbrace{a^{255}-1 \equiv 0 \ (3^2)}_{a} \text{ y } \underbrace{a^{255}-1 \equiv 0 \ (5)}_{b}.$$

porque $(3^2 : 5) = 1$

a) $a^{255}-1 \equiv 0 \ (3^2) \Leftrightarrow a^{255} \equiv 1 \ (3^2)$.

si $3 \mid a \Rightarrow 3^2 \mid a^2 \Rightarrow 3^2 \mid a^2 \cdot a^{253} = a^{255}$.

pero entonces, $a^{255} \equiv 0 \not\equiv 1 \ (3^2) \Rightarrow 3 \nmid a$.

como $3 \nmid a \Rightarrow a^{255} \equiv a^{r_{3^1 \cdot (3-1)}(255)} \equiv a^{r_6(255)}$ (6) (Euler Fermat)

$$255 \equiv 3 \ (6) \Rightarrow a^{255} \equiv a^3 \ (3^2)$$

quiero que $a^3 \equiv 1 \ (3^2)$ → tabla de restos.

a	0	1	2	3	4	5	6	7	8
a^3	0	1	8	0	1	8	0	1	8

mod (9).

Los restos de a^3 mod 3^2 son siempre 0, 1 ó 8, se puede probar fácilmente que se repiten cada 3.

$x \equiv 1\ (9)$, $x \equiv 4\ (9)$ $x \equiv 7\ (9)$

$\hookrightarrow$ $x = 9q + 1$ $x = 9k + 4$ $x = 9j + 7$

$x = 3(3q) + 1$ $x = 3(3k) + 3 + 1$ $x = 3(3j) + 3 + 3 + 1$

$x = 3(3k+1) + 1$ $x = 3(3j+2) + 1$.

en los tres casos llegué a que $x \equiv 1\ (3)$.

(a) $x \equiv 1\ (3)$.

(b) $x^{255} - 1 \equiv 0\ (5) \Leftrightarrow x^{255} \equiv 1\ (5)$

si $5 \mid x \Rightarrow 5 \mid x^{255} \Rightarrow x^{255} \equiv 0 \not\equiv 1\ (5) \Rightarrow 5 \nmid x$.

como $5 \nmid x \Rightarrow x^{255} \equiv x^{r_4(255)} \equiv x^3\ (5)$ (pequeño teorema de Fermat)

quiero que $x^3 \equiv 1\ (5)$. $\rightarrow$ tabla de restos.

x	0	1	2	3	4
x^3	0	1	3	2	4

(mod 5)

$\Rightarrow x^3 \equiv 1\ (5) \Leftrightarrow x \equiv 1\ (5)$

(b) $x \equiv 1\ (5)$.

(a) y (b)

$\left.\begin{array}{l} x \equiv 1\ (3) \\ x \equiv 1\ (5) \end{array}\right\}$ puedo hacer TCH del resto. porque $(3 : 5) = 1$.

$x \equiv 1\ (3) \rightarrow 5 \equiv 2\ (3)$. $\rightarrow$ el inverso es 2. $(2 \cdot 2 \equiv 1\ (3))$

$\Rightarrow$ $x \equiv 1\ (5) \rightarrow 3 \equiv 3\ (5) \rightarrow$ el inverso es 2 $(2 \cdot 3 \equiv 1\ (5))$

$x \equiv 1 \cdot 5 \cdot 2 + 1 \cdot 3 \cdot 2 \equiv 16 \equiv 1\ \underset{5 \cdot 3}{(15)}$.

$\Rightarrow \boxed{x \equiv 1\ (15)}$

RTA $x \equiv 1\ (15)$

Ejercicio 2

a) determinar todos los $m \in \mathbb{N} \mid 3^{108m+15} \equiv 5m \ (19)$.

Como 19 es primo y $19 \nmid 3$

$\Rightarrow 3^{18} \equiv 1 \ (19) \Rightarrow 3^{m} \equiv 3^{r_{18}(m)} \ (19)$. (por el pequeño teorema de Fermat)

Por lo tanto $3^{108m+15} \equiv 3^{r_{18}(108m+15)}$.

$108m+15 \equiv 15 \ (18)$

$\downarrow$

$108 \equiv 0 \ (18)$

Entonces: $3^{108m+15} \equiv 3^{15} \equiv (3^3)^5 \equiv 27^5 \equiv 8^5 \equiv (8^2)^2 \cdot 8 \equiv$

$\equiv (8^2)^2 \cdot 8 \equiv 7^2 \cdot 8 \equiv 11 \cdot 8 \equiv 12 \ (19)$.

$\Rightarrow 3^{108m+15} \equiv 12 \ (19)$.

y además quiero que $3^{108m+15} \equiv 5m \ (19)$.

$\Rightarrow 5m \equiv 12 \ (19)$.

$5 \cdot 4 m \equiv 12 \cdot 4 \ (19)$

$20m \equiv 10 \ (19) \Rightarrow m \equiv 10 \ (19)$.

$\downarrow$

$20 \equiv 1 \ (19)$

RTA $\boxed{m \equiv 10 \ (19)}$

Ejercicio 5

$f = x^4 + x^3 + x^2 + x + 1$ es el polinomio cuyas raíces son las raíces primitivas de G_5.

dem. $G_5 = G_{5\,\text{primitivas}} \dot\cup G_{1\,\text{primitivas}}$ (5 es primo)

$G_5 \to x^5 = 1 \to$ el polinomio es $x^5 - 1 = g$

$G_1 \to x = 1$ y la primitiva de G_1 es 1

entonces si a G_5 le saco la primitiva de G_1 que es 1 tengo un polinomio cuyas raíces son las primitivas de G_5 . $x-1 \mid x^5-1$ → busco un ~~h~~ $x^5-1 = (x-1)\,h$

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

$x^4+x^3+x^2+x+1$ ⇒ polinomio cuyas raíces son raíces primitivas de G_5

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

~~Entonces~~ si $\cancel{x^4+x^3+x^2+x+1} \mid$

Entonces si $x^4+x^3+x^2+x+1 \mid \overbrace{x^{2016}+2x^{1633}-x^{174}+x^{137}+2x^4-x^3+1}^{\text{lo llamo } f}$

las raíces del primer polinomio son raíces del segundo.

⇒ resta ver que si $z \in G_5$ y z es primitiva ⇒ $f(z)=0$.

como z es primitiva de G_5

$$z^{2016}+2z^{1633}-z^{174}+z^{137}+2z^4-z^3+1 = f(z) =$$

$$=(z^5)^{403}.z + 2(z^5)^{366}.z^3 - (z^5)^{34}.z^4 + (z^5)^{27}.z^2 + 2.z^4 - z^3 + 1 = \to \text{como } z^5=1$$

$$=1^{403}.z + 2.1^{366}.z^3 - 1^{34}.z^4 + 1^{27}.z^2 + 2.z^4 - z^3 + 1$$

$$= z + 2z^3 - z^4 + z^2 + 2z^4 - z^3 + 1 = 1 + z + z^2 + z^3 + z^4$$

$$f(z) = 1 + z + z^2 + z^3 + z^4 = 0 \ ?$$

ya dijiste que eran raíces de $1+x+x^2+x^3+x^4$

como z es primitivo de G_5, $\sum_{i=0}^{4} z^i = 0$.

$$\sum_{i=0}^{4} z^i = z^0 + z^1 + z^2 + z^3 + z^4 = 1 + z + z^2 + z^3 + z^4 = 0.$$

Por lo tanto, $f(z) = \sum_{i=0}^{4} z^i = 0$.

como $f(z)=0$ para toda raíz de

$1 + x + x^2 + x^3 + x^4$ ⇒

$$1+x+x^2+x^3+x^4 \mid x^{2016}+2x^{1633}-x^{174}+x^{137}+2x^4-x^3+1.$$