Algebra I
Examen Final (9/08/2017)

Nombre y apellido: [redacted]

Libreta: [redacted] **Carrera:** Lic. en Ciencias de la Computación

1	2	3	4	5	Nota
B	B	B	B	B	10(diez)

1. Sea $X = \{n \in \mathbb{N} \mid n < 10^6\}$ y sea $\mathcal{R} \subset X \times X$ la relación

$$a \mathcal{R} b \iff (2^{20} : a) = (2^{20} : b)$$

Probar que $\mathcal{R}$ es una relación de equivalencia y encontrar el cardinal de la clase de equivalencia de 1000.

2. Sean $A = 40^{10}$ y $B = 44^9$. Hallar todos los $a, b \in \mathbb{N}$ tales que

$$\max\{k \in \mathbb{N} : 2^k \text{ divide a } A^a B^b\} = 726.$$

3. Sea $p > 0$ primo.

   (a) Probar que si $n \in \mathbb{N}$ y $a \in \mathbb{Z}$ entonces $a^{p^n} \equiv a \pmod{p}$.

   (b) Probar que si $f = b_n x^n + b_{n-1} x^{n-1} + \cdots + b_0$ es un polinomio con coeficientes en $\mathbb{N}$ entonces

$$\forall a \in \mathbb{Z}, \quad a^{f(p)} \equiv a^{f(1)} \pmod{p}.$$

   Observación: no es necesario probar el pequeño teorema de Fermat.

4. (a) Probar que si $n \in \mathbb{N}$, el polinomio $x^n - 1$ tiene como raíces a los elementos de G_n.

   (b) Probar que si $n = 2^k$, el polinomio $x^{\frac{n}{2}} - 1$ divide a $x^n - 1$ y que el cociente $\frac{x^n - 1}{x^{\frac{n}{2}} - 1}$ tiene como raíces a las raíces n-ésimas primitivas

5. Sean f y g dos polinomios en $\mathbb{C}[X]$. Probar que si ni f ni g tienen raíces dobles entonces el mínimo común múltiplo $[f : g]$ tampoco tiene raíces dobles.

Nota. Justifique debidamente todas sus afirmaciones y respuestas.

Ejercicio 1

Sea $X = \{m \in \mathbb{N} \mid m < 10^6\}$ y sea $R \subset X \times X$ la relación

$a R b \Leftrightarrow (2^{20} : a) = (2^{20} : b)$.

Probar que es una relación de equivalencia.

Veamos que es reflexiva

R es reflexiva si $\forall z \in X \quad aRa \Leftrightarrow (2^{20} : a) = (2^{20} : a)$ ✓

Veamos que es simétrica

es simétrica si

$\forall a,b \in X \mid a R b \Rightarrow bRa \Leftrightarrow$

$(2^{20} : a) = (2^{20} : b)$ y $(2^{20} : b) = (2^{20} : a)$

Sí, porque $(2^{20} : a) = (a : 2^{20}) = (b : 2^{20}) = (2^{20} : a)$

Veamos que es transitiva.

$\forall a,b,c \in X \mid . aRb \wedge bRc \Rightarrow . aRc.$

$aRb \Leftrightarrow (2^{20} : a) = (2^{20} : b)$

$bRc \Leftrightarrow (2^{20} : b) = (2^{20} : c)$

$\Leftrightarrow (2^{20} : a) = (2^{20} : b) = (2^{20} : c)$

y unicidad del mcd

Br transitividad de la igualdad, $(2^{20} : a) = (2^{20} : c)$

$\Rightarrow . aRc$ R es transitiva ✓

$\Rightarrow$ R es de equivalencia B

Encontrar el cardinal de la clase de equivalencia de 1000

$1000 = 10^3 = (2 \cdot 5)^3 = 2^3 \cdot 5^3$

$a R 1000 \Leftrightarrow (2^{20} : 1000) = (2^{20} : a)$.

$(2^{20} : 1000) = (2^{20} : 2^3 \cdot 5^3) = 2^3$

$\Rightarrow \quad aR1000 \Leftrightarrow \quad 2^3 = (2^{20} : a)$.

$2^3 \mid (2^{20} : a) \Rightarrow 2^3 \mid 2^{20}$ (siempre).

$\Leftrightarrow 2^3 \mid a$

$2^3 \mid a$

Por lo tanto $z = 2^3 \cdot p_1^{\alpha} \cdot p_2^{\beta} \cdot p_3^{\delta} \dots$ (infinitos primos).

pero además, 2^3 es el mayor divisor de 2^{20} y z al mismo tiempo, por lo tanto $2^4 \nmid z$. (si $2^4 \mid z \Rightarrow d = 2^4$. Más!).

$z = 2^3 \cdot 3^{\alpha} \cdot 5^{\beta} \cdot 7^{\delta} \dots$

¿Qué más sé de z? Sé que es natural y menor a 10^6.

$1 \leq z < 10^6$.

$1 \leq 2^3 \cdot 3^{\alpha} \cdot 5^{\beta} \cdot 7^{\delta} \dots < 10^6$.

$0{,}125 = \frac{1}{2^3} \leq 3^{\alpha} \cdot 5^{\beta} \cdot 7^{\delta} \dots < \frac{10^6}{2^3} = 125\,000$.

$1 \leq 3^{\alpha} \cdot 5^{\beta} \cdot 7^{\delta} \dots \leq 124.999$

y además, $2 \nmid \underbrace{3^{\alpha} \cdot 5^{\beta} \cdot 7^{\delta} \dots}$

es decir, ese número puede ser cualquier número impar entre 1 y 124.999.

Por lo tanto, como tengo $\left[\frac{124.999}{2}\right] = 62499$ números pares hasta 124999. $\Rightarrow$ hay $124999 - 62499 = 62500$ números impares desde 1 hasta 124999.

En conclusión, el cardinal de la clase de equivalencia de 1000 es 62500.

B

[redacted]

214 hojas

Ejercicio 3

$p > 0$

(a) probar que si $m \in \mathbb{N}$ y $a \in \mathbb{Z}$ entonces $a^{p^m} \equiv a \ (p)$.

si $p \mid a \iff a \equiv 0 \ (p) \Rightarrow a^{p^m} \equiv 0^{p^m} \equiv 0 \equiv a \ (p)$ ✓.

si $p \nmid a$ puedo usar PTF.

$a^{p^m} \equiv a^{r_{(p-1)}(p^m)}$

se que $p-1 \mid p-1 \iff p \equiv 1 \ (p-1)$

$p^m \equiv 1^m \equiv 1 \ (p-1)$.

$a^{r_{p-1}(p^m)} \equiv a^1 \equiv a \ (p)$. ✓ B

(b) dado $f = b_m x^m + b_{m-1} x^{m-1} + \dots + b_1 x + b_0$

probar que $\forall a \in \mathbb{Z} \quad a^{f(p)} \equiv a^{f(1)} \ (p)$.

si $p \mid a \Rightarrow a^{f(p)} \equiv 0 \equiv 0^{f(1)} \equiv a^{f(1)} \ (p)$.

$\iff f(p) \neq f(1) \neq 0$. pero se que como $f \in \mathbb{N}$ y $p > 0$ y $1 > 0 \Rightarrow f(1) > 0$ y $f(p) > 0$ (son ole positivos no puede dar 0). ✓

si $p \nmid a \Rightarrow$ podemos usar PTF

$a^{f(p)} \equiv a^{r_{p-1}(f(p))}$

$f(p) = b_m \cdot p^m + b_{m-1} \cdot p^{m-1} + \dots + p \cdot b_1 + b_0$

y se que $p^n \equiv 1 \ (p-1)$ (probado en ítem a)

$\Rightarrow f(p) = b_m \cdot p^m + b_{m-1} \cdot p^{m-1} + \dots + p \cdot b_1 + b_0 \equiv$ ⇕ $p \equiv 1 \ (p-1)$

$b_m \cdot 1^m + b_{m-1} \cdot 1^{m-1} + \dots + 1 \cdot b_1 + b_0 \equiv$

$b_m + b_{m-1} + \dots + b_1 + b_0 \ (p-1)$.

y este resto es efectivamente $f(1)$.

$f(1) = b_m \cdot 1^m + \dots + b_0 = b_m + b_{m-1} + \dots b_1 + b_0$

por lo tanto.

$a^{f(p)} \equiv a^{r(f(p))} \equiv a^{f(1)} \pmod{p}$ B

Ejercicio 4

(a) Si $n \in \mathbb{N} \Rightarrow x^n - 1$ tiene como raíces a todo $z \in G_n$.

Recuerdo que $z \in G_n \Leftrightarrow z^n = 1$.

$\Rightarrow$ $f = x^n - 1 = 0 \Leftrightarrow x^n = 1$. y los x que cumplen esto, son los $z \in G_n$ porque

$f(z) = z^n - 1 = 1 - 1 = 0$ ✓.

(b) Si $n = 2^k \Rightarrow$ (los divisores de n son potencias de 2. (2^d con $0 \leq d \leq k$)

Por lo tanto como G_n es la unión de los primitivos de todo G_t con $t \mid n \Rightarrow$

$G_n = G_{2^k} = G_{2^0}^* \cup G_{2^1}^* \cdots \cup G_{2^k}^*$

esto vale para 2^{k-1} también (vale para cualquier potencia de 2)

$G_{2^{k-1}} = G_{2^0}^* \cup G_{2^1}^* \cdots \cup G_{2^{k-1}}^*$

Vemos que $G_n = G_{2^k} = G_{2^{k-1}} \cup G_{2^k}^*$

esto se traduce a que G_n tiene a todos los $z \in G_{2^{k-1}}$ y además a los primitivos de $G_{2^k}^*$

$\Rightarrow$. Si $z \in G_{2^{k-1}} \Rightarrow z \in G_{2^k} \Leftrightarrow z^{2^k} = 1$. y $z^{2^{k-1}} = 1$

$g = x^{\frac{n}{2}} - 1 = x^{2^{k-1}} - 1$ tiene como raíces a $G_{2^{k-1}}$ (por (a))

Por lo tanto, todas las raíces de g son también raíces de $f = x^n - 1 = x^{2^k} - 1$ y que f tiene como raíces a $G_n = G_{2^k}$

[redacted] | 3 | 4 hojas

f se puede escribir como $f = g \cdot h$.

(porque $g \mid f$: ya que todas las raíces de g son raíces de f) y la multiplicidad es 1 en todas las raíces

Resp ver. que h tiene como raíces a las n-ésimas primitivas.

Como dije antes, G_m es la unión de $G_{2^{k-1}}$ y los primitivos de G_m, por lo tanto, h sí o sí tiene como raíces a las n-ésimas primitivas. (al olvidar a f por $G_{2^{k-1}}$, es decir, las que no son primitivas, quedan las primitivas).

B

Ejercicio 5

f y $g \in \mathbb{C}[x]$, ni f ni g tienen raíces dobles.

Por lo tanto, en su forma factorizada, cada factor es simple (porque si α es raíz multiple $\Rightarrow$ $(x-\alpha)^2 \mid f$.) sabemos que

f es de la forma $F \cdot (x-\alpha)(x-\beta)(x-\delta)\dots$

con F = coef ppal(f), G = coef ppal(g)

y g es de la forma $G \cdot (x-a)(x-b)(x-c)\dots$

($\forall \alpha \mid f(\alpha)=0 \Rightarrow x-\alpha \mid f$ pero $(x-\alpha)^2 \nmid f$ y lo mismo vale para g).

entonces, el mínimo común múltiplo entre f y g es:

$[f:g] = [(x-\alpha)(x-\beta)(x-\delta)\ldots : (x-a)(x-b)(x-c)\ldots]$

y esto es igual a cada posible factor del tipo $(x-t)$ elevado a la máxima potencia a la que aparece entre f y g. Si $(x-t)$ divide a f => la máxima potencia es 1, porque es cero simple. Lo mismo pasa para g, si $(x-t) \mid g \Rightarrow (x-t)$ está elevado a la uno.

y si $(x-t) \mid g$ y $(x-t) \mid f$

y en ambos es simple $\Rightarrow (x-t) \mid [f:g]$ pero $(x-t)^2 \nmid [f:g]$.

Por lo tanto $[f:g] = (x-\alpha)(x-\beta)(x-\delta)\ldots(x-a)(x-b)(x-c)\ldots$ (tiene solo raíces simples)

B

[redacted] [redacted] 414 hojas

Ejercicio 2

$A = 40^{10}$ $B = 44^7$, hallar $a, b \in \mathbb{N}$ /

$\max \{ k \in \mathbb{N} \mid 2^k \text{ divide a } A^a \cdot B^b \} = 726$.

$\Leftrightarrow 2^{726} \mid A^a \cdot B^b$ pero $2^{727} \nmid A^a \cdot B^b$

$A^a \cdot B^b = (40^{10})^a \cdot (44^7)^b$ $40 = 2^3 \cdot 5$

$= (2^3 \cdot 5)^{10a} \cdot (2^2 \cdot 11)^{7b}$ $44 = 2^2 \cdot 11$

$= 2^{30a} \cdot 5^{10a} \cdot 2^{14b} \cdot 11^{7b}$

$= 2^{30a+14b} \, 5^{10a} \cdot 11^{7b} \Rightarrow 2^{726} \mid A^a \cdot B^b \Leftrightarrow$ (*)

$2^{726} \mid 2^{30a+14b}$ y $2^{727} \nmid 2^{30a+14b}$ ✓

$\Leftrightarrow 726 = 30a + 14b$ ✓

$(30 : 14) = 6$ y $6 \mid 726 \Rightarrow$ (es una ecuación diofántica)

$\frac{726}{6} = \frac{30}{6} \cdot a + \frac{14}{6} \cdot b$

$121 = 5a + 7b$

Una solución particular es:

$a_0 = 23$ $b_0 = 2$ ✓

$\Rightarrow a = 7k + 23$ $b = -5k + 2$ ✓

pero además a y b son naturales.

$7k + 23 \geq 1$ y $-5k + 2 \geq 1$.

$k \geq -\frac{22}{7} = -7,33$ $k \leq \frac{1}{5} = 0,2$

$-7 \leq k \leq 0$

Posibles a y b:

$k = 0 \Rightarrow a = 23$ y $b = 2$

$k = -1 \Rightarrow a = 20$ y $b = 7$

$k = -2 \Rightarrow a = 17$ y $b = 12$

$k = -3 \Rightarrow a = 14$ y $b = 17$

$k = -4 \Rightarrow a = 11$ y $b = 22$

$k = -5 \Rightarrow a = 8$ y $b = 27$

$k = -6 \Rightarrow a = 5$ y $b = 32$

$k = -7 \Rightarrow a = 2$ y $b = 37$

B

(*) $2^{276} \mid 2^{30a+14b} \Rightarrow$

$30a+18b \nmid 726$

$2^{727} \times 30a+18b \Rightarrow 30a+18b < 727$

$\Rightarrow 30a+18b = 276.$