

CS041 Matemática Discreta Aplicada

Examen Parcial 2

Nombre: David Lora

Resumen:

Ejercicio:	1	2	3	4	5	6	7	8	Total
Puntos:	13	13	13	13	13	13	11	11	100
Resultado:									

Parte I: Resuelva los siguientes ejercicios de forma clara y ordenada, dejando constancia de todo su procedimiento.

1. (13 puntos) Encuentre el $\text{mcd}(2689, 1369)$.

2. (13 puntos) Manuel tiene dos contenedores. Un contenedor puede almacenar 23 ml y el otro 21 ml. Explique, ¿cómo puede usar Manuel estos contenedores para medir exactamente 1 ml? Justifique su respuesta usando un procedimiento no exhaustivo.

3. (13 puntos) Indique para qué valor (o valores) de k tiene solución la ecuación diofantina:

$$128x + 60y = k$$

4. (13 puntos) Si $a, b \in \mathbb{Z}^+$ con $a = 420$, $\text{mcd}(a, b) = 2$ y $\text{mcm}(a, b) = 5460$, determine el valor de b .

5. (13 puntos) Encuentre todas las soluciones de la ecuación diofantina:

$$121x + 74y = 208$$

6. (13 puntos) Usando el algoritmo de exponentiación modular, calcule:

$$9^{29} \in \mathbb{Z}_{13}$$

Parte II: Suponga que cada letra del alfabeto (y el espacio) se puede codificar con los dígitos según la siguiente tabla:

U = 00	D = 04	H = 08	L = 12	O = 16	S = 20	W = 24
A = 01	E = 05	I = 09	M = 13	P = 17	T = 21	X = 25
B = 02	F = 06	J = 10	N = 14	Q = 18	U = 22	Y = 26
C = 03	G = 07	K = 11	Ñ = 15	R = 19	V = 23	Z = 27

7. (11 puntos) Utilice el cifrado de César ponderado con clave $k = 5$ y $d = 11$ para encriptar el mensaje: ATACAR AL AMANECER.
8. (11 puntos) Se ha interceptado el siguiente mensaje UOWFGNFDNPNDKXNFOWPOWNWKN. Si se sabe que se ha utilizado el cifrado César ponderado con $k = 7$ y $d = 6$, descifre el mensaje.

$$a = 7 \mod(28) \quad \text{mcd}(28, 7)$$

$$a \cdot a^{-1} \equiv_2 1$$

$$7 \cdot a^{-1} \equiv_{28}$$

$$1 \equiv_{28} 29 \equiv_{28}$$

Parcial # 2

David Corzo 20140432

$$\textcircled{1} \quad \text{mcd}(2686, 1369)$$

$$2686 = 1369 \cdot \boxed{1} + 1317$$

$$\text{mcd}(1369, 1317)$$

$$1369 = 1317 \cdot \boxed{1} + 52$$

$$\text{mcd}(1317, 52)$$

$$1317 = 52 \cdot \boxed{25} + 17$$

$$\text{mcd}(52, 17)$$

$$52 = 17 \cdot \boxed{3} + 1$$

$$\text{mcd}(17, 1)$$

$$17 = 1 \cdot \boxed{17} + 0$$

$$\text{mcd}(1, 0)$$

$$\text{mcd}(2686, 1369) = 1 \quad \checkmark$$

$\textcircled{2}$ Contenedor₁ = 23 ml
 Contenedor₂ = 21
 # Primera saquemos el mcd de 23, 21

$$\text{mcd}(23, 21)$$

$$23 = 21 \cdot \boxed{1} + 2$$

$$\text{mcd}(21, 2)$$

$$21 = 2 \cdot \boxed{10} + 1$$

$$\text{mcd}(2, 1)$$

$$1 = 1 \cdot \boxed{1} + 0$$

$$\text{mcd}(1, 0)$$

$$23x + 21y = 1$$

$\textcircled{3}$ Encuentre valores de K.

$$128x + 60y = K$$

$$\text{mcd}(128, 60) \quad \text{Es correcto.}$$

La ecuación tiene $128 = 60 \cdot \boxed{2} + 8$ que 7 módulos
 solución si tal $\text{mcd}(60, 8)$ no puede tener
 K está representado inversa, pero a fuerza
 por múltiplos de 60 = $8 \cdot \boxed{7} + 4$ bruto es posible
~~4!~~ describirlo.

$$\text{mcd}(8, 4)$$

$$8 = 4 \cdot \boxed{2} + 0$$

$$\text{mcd}(4, 0)$$

$$\text{mcd}(128, 60) = 4$$

$\textcircled{4}$

$$a, b \in \mathbb{Z}^+ ; a = 420$$

$$\text{mcd}(a, b) = 2$$

$$\text{mcm}(a, b) = 5460$$

$$\text{mcd}(a, b) \text{ mcm}(a, b) = a \cdot b$$

$$\frac{(2)(5460)}{420} = b$$

$$\frac{2 \cdot 5460}{210} = b$$

$$\frac{5460}{210} = b$$

$$b = 26 \quad \checkmark$$

Ejercicio	1	2	3	4	5	6	7	8	Final
Puntos	13	13	13	13	13	13	11	5	94

⑥ Algoritmo de exponenteación modular:

$$9^{24} \in \mathbb{Z}_{13}$$

Escribir 29 en binario.

$$29_2 = \begin{array}{r} 1 & 1 & 1 & 0 & 1 \\ + & 3 & 2 & 1 & 0 \end{array}$$

$$29 = 2^4 + 2^3 + 2^2 + 2^0 \quad \checkmark$$

Bits	a^{2^n}	$a^2 \text{ mod}(n)$	
0 1	$9^{2^0} = 9 \equiv_{13} 9$	$9^2 = 81 \equiv_{13} 3$	
1 0	$9^{2^1} = 9^2 \equiv_{13} 3$	$3^2 \equiv_{13} 9$	
2 1	$9^{2^2} = 9^4 \equiv_{13} 9$	$9^2 \equiv_{13} 3$	
3 1	$9^{2^3} = 9^8 \equiv_{13} 3$	$3^2 \equiv_{13} 9$	
4 1	$9^{2^4} = 9^{16} \equiv_{13} 9$	$9^2 \equiv_{13} 3$	

$$\begin{aligned} \frac{29}{2} &= 14 + \frac{1}{2} \\ \frac{14}{2} &= 7 + \frac{0}{2} \\ \frac{7}{2} &= 3 + \frac{1}{2} \\ \frac{3}{2} &= 1 + \frac{1}{2} \\ \frac{1}{2} &= 0 + \frac{1}{2} \\ 11101 \end{aligned}$$

$$f_0(81 \div 13) = 6$$

$$13 \cdot 6 = 78$$

$$81 - 78 = 3$$

$$\begin{aligned} 9^{29} &= 9^4 \cdot 9^3 \cdot 9^2 \cdot 9^0 \\ &\equiv_{13} 9 \cdot 3 \cdot 9 \cdot 9 \\ &\equiv_{13} 9^2 \cdot 9 \cdot 3 \\ &\equiv_{13} 3 \cdot 9 \cdot 3 \equiv_{13} 3^2 \cdot 9 \\ &\equiv_{13} 9 \cdot 9 \equiv_{13} 9^2 \equiv_{13} \boxed{3} \end{aligned}$$

②

~~RES~~

$$\text{contenedor}_1 = 23$$

$$\text{contenedor}_2 = 21$$

$$\text{mcd}(23, 21)$$

$$23 = 21 \cdot \boxed{1} + 2$$

$$\text{mcd}(21, 2)$$

$$21 = 2 \cdot \boxed{10} + 1$$

$$\text{mcd}(2, 1)$$

$$2 = 1 \cdot \boxed{2} + 0$$

$$\text{mcd}(1, 0)$$

$$\# El \text{ mcd}(23, 21) = 1$$

$$23x + 21y = 1$$

Bézout reversible

$$21 - 2 \cdot 10 = 1$$

$$21 - (23 - 21) \cdot 10 = 1$$

$$21 - 10(23 - 21) = 1$$

$$21 - 10 \cdot 23 + 10 \cdot 21 = 1$$

$$-10 \cdot 23 + 11 \cdot 21 = 1$$

Manuel debe llenar 11 veces el de 21 ml & ~~después vaciar~~ 10 veces el de 23 ml.

La solución es $x = 7(47 - 47) - 4 \cdot 47 = 7$
en que $x \& y = 7 \cdot 47 - 7 \cdot 47 - 4 \cdot 47 = 1$

+ tienen que ser de la forma $7 \cdot 47 - 11 \cdot 47 = 1$

$$y = \frac{7 \cdot 47 - 11 \cdot 47}{11} + k \\ 7 \cdot 74 - 11(121 - 74) = 1 \\ 7 \cdot 74 - 11 \cdot 121 + 11 \cdot 74 = 1 \\ 128 \cdot 74 - 11 \cdot 121 = 1$$

(5) \rightarrow supongo que es un 5...

$$121x + 74y = 208$$

$$\text{mcd}(121, 74)$$

$$121 = 74 \cdot \boxed{1} + 47$$

$$\text{mcd}(74, 47)$$

$$74 = 47 \cdot \boxed{1} + 27 \checkmark$$

$$\text{mcd}(47, 27)$$

$$47 = 27 \cdot \boxed{1} + 20 \checkmark$$

$$\text{mcd}(27, 20)$$

$$27 = 20 \cdot \boxed{1} + 7 \checkmark$$

$$\text{mcd}(20, 7)$$

$$20 = 7 \cdot \boxed{2} + 6 \checkmark$$

$$\text{mcd}(7, 6)$$

$$7 = 6 \cdot \boxed{1} + 1 \checkmark$$

$$\text{mcd}(6, 1)$$

$$6 = 1 \cdot \boxed{6} + 0$$

$$\text{mcd}(1, 0)$$

$$\text{mcd}(121, 74) = 1 \checkmark$$

$$7 - 6 = 1$$

$$7 - (20 - 7 \cdot 2) = 1$$

$$7 - 20 + 7 \cdot 2 = 1$$

$$3 \cdot 7 - 20 = 1$$

$$3(27 - 20) - 20 = 1$$

$$3 \cdot 27 - 3 \cdot 20 - 20 = 1$$

$$3 \cdot 27 - 4 \cdot 20 = 1$$

$$3 \cdot 27 - 4(47 - 27) = 1$$

$$3 \cdot 27 - 4 \cdot 47 + 4 \cdot 27 = 1$$

$$7 \cdot 27 - 4 \cdot 47 = 1$$

⑦ Cesar ponderado $k = 5$; $d = 11$
 "ATACAR AL AMANECER"

Original

$$E(x) = 5x + 11$$

$$\begin{aligned}
 A &= 1 \rightarrow 16 \equiv_{28} 16 \rightarrow 0 \\
 T &= 21 \rightarrow 116 \equiv 4 \rightarrow D \\
 A &= 1 \rightarrow 16 \equiv 16 \rightarrow 0 \\
 C &= 3 \rightarrow 26 \equiv 26 \rightarrow Y \\
 A &= 1 \rightarrow 16 \equiv 16 \rightarrow 0 \\
 R &= 19 \rightarrow 106 \equiv 22 \rightarrow U \\
 L &= 0 \rightarrow 11 \equiv 11 \rightarrow K \\
 A &= 1 \rightarrow 16 \equiv 16 \rightarrow 0 \\
 L &= 12 \rightarrow 71 \equiv 15 \rightarrow N \\
 L &= 0 \rightarrow 11 \equiv 11 \rightarrow K \\
 A &= 1 \rightarrow 16 \equiv 16 \rightarrow 0 \\
 M &= 13 \rightarrow 76 \equiv 20 \rightarrow S \\
 A &= 1 \rightarrow 16 \equiv 16 \rightarrow 0 \\
 N &= 14 \rightarrow 81 \equiv 25 \rightarrow X \\
 E &= 5 \rightarrow 36 \equiv 8 \rightarrow H \\
 C &= 3 \rightarrow 26 \equiv 26 \rightarrow Y \\
 E &= 5 \rightarrow 36 \equiv 8 \rightarrow H \\
 R &= 19 \rightarrow 106 \equiv 22 \rightarrow U
 \end{aligned}$$

$$U = 12$$

$$D = 16$$

$$W = 24$$

$$F = 6$$

$$G = 7$$

$$N = 14$$

$$P = 6$$

$$D = 4$$

$$N = 14$$

$$P =$$

$$N =$$

$$D =$$

$$K =$$

$$X =$$

$$N =$$

$$F =$$

$$D =$$

$$W =$$

$$P =$$

$$D =$$

$$W =$$

$$N =$$

$$W =$$

$$K =$$

$$N =$$

$$D(x) = (x - 6) \cdot 7^{-1}$$

Dado que 7 módulo 28 no tiene inversa
 \therefore no se puede desencriptar.

$$7 \in \mathbb{Z}_{28}$$

$$28 = 7 \cdot \boxed{4} + 0$$

$$\text{mcd}(7, 0)$$

No hay inversos