

**Universidad de la República - Facultad de Ingeniería - IMERL: Matemática  
Discreta 2, semipresencial**

PRIMER PARCIAL - 25 DE SETIEMBRE DE 2017. DURACIÓN: 3 HORAS

Nº de parcial	Cédula	Apellido y nombre

Para cada pregunta o ejercicio, deben presentar claramente el razonamiento y cálculos realizados para obtener su respuesta final. Si una implicancia es válida debido a algún teorema, proposición o propiedad, deben especificarlo (nombre del teorema, lema, etc.) Presentar una respuesta final a la pregunta sin justificación carece de validez.

**Ejercicio 1.**

- a. Resolver el sistema

$$\begin{cases} x \equiv 8 \pmod{11} \\ x \equiv 11 \pmod{16} \end{cases},$$

- b. Probar que si  $\text{mcd}(a, n) = 1$  entonces  $a$  es invertible módulo  $n$ .  
c. Hallar el inverso de 7 módulo 11.  
d. Hallar  $x \in \{0, 1, \dots, 10\}$  tal que  $x \equiv 7^{139} \pmod{11}$ .  
e. Hallar  $x \in \{0, 1, \dots, 15\}$  tal que  $x \equiv 3^{139} \pmod{16}$ .  
f. Hallar todos los  $x \in \mathbb{Z}$  tal que  $x \equiv 51^{139} \pmod{176}$ .

**Ejercicio 2.**

- a. Sean  $0 \neq a, b \in \mathbb{Z}$ , probar que  $\text{mcd}(a, b) = \min\{c > 0 : c = ax + by \text{ con } x, y \in \mathbb{Z}\}$ .  
b. Sean  $a, b \in \mathbb{Z}$  tales que  $\text{mcd}(a, b) = 1$ .  
i) Probar que si  $p$  es un primo divisor común de  $(a + 2b)$  y  $ab$ , entonces  $p = 2$ .  
ii) Hallar  $\text{mcd}(a + 2b, ab)$  discutiendo según la paridad de  $a$ .

**Ejercicio 3.**

- a. Hallar todos  $a, b \in \mathbb{N}$  tales que  $\text{mcd}(a, b) = 12$ ,  $a$  tiene 15 divisores positivos y  $b$  tiene 12.  
b. Sea  $(p_n)$  la sucesión de los números primos,  $p_1 = 2$ ,  $p_2 = 3$ , etc. Probar que para todo  $n > 1$  y todo  $k = 1, \dots, n - 1$ , se tiene que

$$p_1 p_2 \cdots p_k + p_{k+1} p_{k+2} \cdots p_n \geq p_{n+1}.$$

**Universidad de la República - Facultad de Ingeniería - IMERL: Matemática  
Discreta 2**

SOLUCIÓN PRIMER PARCIAL - 27 DE ABRIL DE 2017.

**Ejercicio 1.** Encontrar todos los  $a, b \in \mathbb{N}$  tales que  $a + b = 407$  y  $\text{mcm}(a, b) = 210 \text{mcd}(a, b)$ .

**Solución:** Sean  $d = \text{mcd}(a, b)$  y  $a = da^*$ ,  $b = db^*$ . Como

$$d(a^* + b^*) = a + b = 11 \cdot 37$$

entonces  $d \mid 407$  y  $d \in \{1, 11, 37, 407\}$ .

Por otro lado, como  $\text{mcm}(a, b) \text{mcd}(a, b) = ab$ , tenemos

$$d^2 a^* b^* = ab = 210 \text{mcd}(a, b)^2 = 2 \cdot 3 \cdot 5 \cdot 7 d^2.$$

Por lo tanto

$$a^* b^* = 2 \cdot 3 \cdot 5 \cdot 7.$$

Recordemos que  $\text{mcd}(a^*, b^*) = 1$  por lo tanto  $a^* \in \{1, 2, 3, 5, 6, 7, 10, 14, 15, 21, 30, 35, 42, 70, 105, 210\}$ .  
Veamos para que  $d$  hay alguna solución.

- Si  $d = 1$  entonces  $a^* + b^* = 407$ , y mirando entre las opciones para  $a^*$  y  $b^*$  vemos que ninguna llega a sumar 407.
- Si  $d = 11$  entonces  $a^* + b^* = 37$ , dentro de las opciones para  $a^*$  y  $b^*$ , recordar que  $a^* b^* = 210$ , las únicas que funcionan son  $(a^*, b^*) = (7, 30)$  y  $(a^*, b^*) = (30, 7)$ .
- Si  $d = 37$  entonces  $a^* + b^* = 11$ , ninguna de las opciones para  $a^*$  y  $b^*$  funcionan.
- Si  $d = 407$  entonces  $a^* + b^* = 1$  y ninguna de las opciones para  $a^*$  y  $b^*$  funcionan.

Por lo tanto las soluciones son  $(a, b) = (7 \cdot 11 = 77, 30 \cdot 11) = (77, 330)$  y  $(a, b) = (330, 77)$ .

**Ejercicio 2.** Sean  $a, b, c \in \mathbb{Z}$  con  $(a, b) \neq (0, 0)$ . Probar que la ecuación diofántica

$$ax + by = c$$

tiene solución si y solo si  $\text{mcd}(a, b) \mid c$ .

**Solución:** Sea  $d = \text{mcd}(a, b)$ . Como  $(a, b) \neq (0, 0)$  tenemos que  $d \neq 0$ .

( $\longrightarrow$ ) Si la ecuación tiene solución, entonces existen  $x_0, y_0 \in \mathbb{Z}$  tales que  $ax_0 + by_0 = c$ . Como  $d \mid a$  y  $d \mid b$ , entonces  $d \mid ax_0 + by_0 = c$ .

( $\longleftarrow$ ) Supongamos que  $d \mid c$  y veamos que la ecuación tiene solución:

Como  $d \mid c$  existe  $k \in \mathbb{Z}$  tal que  $c = dk$ . Por la identidad de Bezout existen  $x', y' \in \mathbb{Z}$  tales que  $ax' + by' = d$ . Multiplicando ambos lados de la ecuación por  $k$ , obtenemos que  $a(x'k) + b(y'k) = c$ , y por lo tanto  $x_0 = x'k$ ,  $y_0 = y'k$  es una solución de la ecuación  $ax + by = c$ .

**Ejercicio 3.**

- a. Hallar el menor  $x$  natural que verifica

$$\begin{cases} x \equiv 6 & (\text{mód } 13) \\ x \equiv 62 & (\text{mód } 103) \end{cases}$$

- b. Si  $(n, e) = (1339, 311)$  calcular  $E(11)$ , donde  $E$  es la función de cifrado del criptosistema RSA con clave pública  $(n, e)$ .
- c. Sabiendo que  $1339 = 13 \cdot 103$  calcular la función de descifrado  $D$  del criptosistema RSA para la clave pública  $(n, e)$  de la parte anterior.
- d. Sean  $n = p \cdot q$ , con  $p, q$  primos, y  $0 < e < \varphi(n)$  con  $\text{mcd}(e, \varphi(n)) = 1$ . Dadas las funciones de cifrado  $E$  y descifrado  $D$  del criptosistema RSA para  $(n, e)$ , probar que  $D(E(x)) \equiv x \pmod{n}$  cuando  $\text{mcd}(x, n) = 1$ .

**Solución:**

- a. Sabemos que el sistema tiene solución por TCR ya que 13 y 103 son coprimos. Combinando las dos congruencias obtenemos que

$$x = 62 + 103k \equiv 6 \pmod{13}.$$

Ahora, como  $103 \equiv -1 \pmod{13}$  y  $62 \equiv -3 \pmod{13}$  vemos que  $k = 4$  y  $x \equiv 474 \pmod{13 \cdot 103}$ . Por lo tanto, la solución buscada es

$$x = 474.$$

- b. Tenemos que calcular  $x \equiv 11^{311} \pmod{1339}$ , con  $0 \leq x < 1339$ . Como  $1339 = 13 \cdot 103$  y TCR, esto es equivalente a resolver el sistema

$$\begin{cases} x \equiv 11^{311} & (\text{mód } 13) \\ x \equiv 11^{311} & (\text{mód } 103) \end{cases}, x \in \mathbb{Z}.$$

En la primer congruencia podemos aplicar el teorema de Euler ya que 11 y 13 son coprimos. Como  $311 \equiv -1 \pmod{12}$  y  $\varphi(13) = 12$  tenemos que

$$11^{311} \equiv 11^{-1} \pmod{13} \equiv (-2)^{-1} \pmod{13} \equiv -7 \pmod{13} \equiv 6 \pmod{13}.$$

Para la segunda congruencia también podemos aplicar Euler y como  $311 \equiv 5 \pmod{102}$  entonces

$$11^{311} \equiv 11^5 \pmod{103} \equiv 18 \cdot 18 \cdot 11 \pmod{103} \equiv 15 \cdot 11 \pmod{103} \equiv 62 \pmod{103}.$$

Entonces, por lo visto en la primer parte del ejercicio vemos que

$$E(x) = 474.$$

- c. Para hallar  $D$  tenemos que hallar  $0 \leq d < \varphi(n) = 1224$  tal que  $e \cdot d \equiv 1 \pmod{1339}$ . O sea, hallar el inverso de  $e$  módulo 1339. Para ello aplicamos el algoritmo extendido de Euclides para hallar la identidad de Bezout

$$1224 \cdot (-140) + 311 \cdot 511 = 1,$$

y por lo tanto  $d = 551$  y  $D(y) = y^{551} \pmod{1339}$ .

- d. Como  $D(E(x)) \equiv x^{ed} \pmod{n}$ , debemos probar que  $x^{ed} \equiv x \pmod{n}$ . Por la construcción del sistema RSA tenemos que  $ed \equiv 1 \pmod{\varphi(n)}$ , es decir que  $ed = \varphi(n)k + 1$ .

Ahora como  $\text{mcd}(x, n) = 1$ , el Teorema de Euler dice que

$$x^{\varphi(n)} \equiv 1 \pmod{n}.$$

Entonces

$$x^{ed} = x^{\varphi(n)k+1} = (x^{\varphi(n)})^k \cdot x \equiv 1^k \cdot x \equiv x \pmod{n}.$$

**Ejercicio 4.** Demostrar la siguiente versión del teorema chino del resto.

Sean  $m_1, m_2$  enteros coprimos y  $a_1, a_2 \in \mathbb{Z}$ , entonces el sistema

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \end{cases}, x \in \mathbb{Z},$$

tiene solución y es única módulo  $m_1 m_2$ .

**Solución:** La primer congruencia es equivalente a que existe  $s \in \mathbb{Z}$  tal que  $x = a_1 + m_1 s$ , y la segunda congruencia a que exista  $t \in \mathbb{Z}$  tal que  $x = a_2 + m_2 t$ . Igualando ambas ecuaciones obtenemos

$$a_1 + m_1 s = a_2 + m_2 t,$$

o lo que es lo mismo

$$m_1 s - m_2 t = a_2 - a_1.$$

Como  $\text{mcd}(m_1, m_2) = 1$ , esta ecuación siempre tiene solución en  $\mathbb{Z}$  (por el ejercicio 2). Ahora si  $s_0, t_0 \in \mathbb{Z}$  es una solución, tenemos que  $x = a_1 + m_1 s_0 = a_2 + m_2 t_0$  es una solución al sistema de congruencias planteado.

Para ver la unicidad de la solución módulo  $m_1 m_2$ , consideremos  $x_0$  y  $x_1$  dos soluciones. Entonces  $x_0 \equiv x_1 \pmod{m_1}$  y  $x_0 \equiv x_1 \pmod{m_2}$ . Dicho de otro modo,  $m_1 \mid (x_0 - x_1)$  y  $m_2 \mid (x_0 - x_1)$ . Pero como  $\text{mcd}(m_1, m_2) = 1$  esto implica que  $m_1 m_2 \mid (x_0 - x_1)$ , es decir que  $x_0 \equiv x_1 \pmod{m_1 m_2}$ .

Universidad de la República - Facultad de Ingeniería - IMERL  
Matemática Discreta 2, semipresencial

SOLUCIÓN PRIMER PRUEBA  
9 DE SETIEMBRE DE 2016

**Ejercicio 1.**

a. Resolver la ecuación diofántica:

$$738x + 621y = 45$$

b. ¿Existen enteros positivos  $x, y$  tales que  $738x + 621y = 49563$ ? Justifique la respuesta.

Solución:

a. La ecuación diofántica  $738x + 621y = 45$  es equivalente, dividiendo todos los coeficientes por 9, a la ecuación  $82x + 69y = 5$ . Como el  $\text{mcd}(82, 69) = 1$  entonces esta ecuación tiene solución en los enteros. Buscaremos primeros los valores  $x_0, y_0 \in \mathbb{Z}$  tales que:

$$(*) \quad 82x_0 + 69y_0 = 1 \text{ (Lema de Bézout).}$$

Tenemos:

- $82 = 69 \times 1 + 13$ ;
- $69 = 13 \times 5 + 4$ ;
- $13 = 4 \times 3 + 1$ .

Entonces  $1 = 13 - 4 \times 3 = 13 - (69 - 13 \times 5) \times 3 = 13 \times 16 - 69 \times 3 = (82 - 69) \times 16 - 69 \times 3 = 82 \times 16 - 69 \times 19$ . O sea  $1 = 82 \times 16 - 69 \times 19 = 82 \times 16 + 69 \times (-19)$ . Por lo tanto  $x_0 = 16$  e  $y_0 = -19$ , son una solución de la ecuación (\*).

Luego, tomando  $x_1 = 5 \times 16 = 80$  e  $y_1 = 5 \times (-19) = -95$  obtenemos una solución de la ecuación  $82x + 69y = 5$  pues  $82 \times 80 - 69 \times 95 = 5$ . Ahora, multiplicando por 9 volvemos a la ecuación original:  $738x + 621y = 45$  y tenemos:  $738 \times 80 - 621 \times 95 = 45$ .

Entonces todas las soluciones de la ecuación  $738x + 621y = 45$  están dadas por:

$$\{(x_t, y_t) / x_t = 80 + 69t, y_t = -95 - 82t, \text{ con } t \in \mathbb{Z}\},$$

pues  $69 = \frac{621}{9}$  y  $82 = \frac{738}{9}$ , siendo  $\text{mcd}(738, 621) = 9$ .

b. La respuesta es NO. La sección 1.6 “*Problema de los Sellos*” es la clave.

La Proposición 1.6.1 dice: Sean  $a > 1, b > 1$  enteros, primos entre sí. Entonces no hay enteros  $x, y$ , no negativos tal que  $ax + by = a \times b - a - b$ .

A la vez, la Proposición 1.6.2 dice: Sean  $a$  y  $b$  enteros positivos primos entre sí. Si  $n \geq a \times b - a - b + 1$ , entonces existen enteros no negativos  $x, y$  tales que:  $ax + by = n$ .

Como  $\text{mcd}(738, 621) = 9$  divide a 49563 entonces la ecuación  $738x + 621y = 49563$  es equivalente a  $82x + 69y = 5507$ . Pero es clave, según las proposiciones citadas, calcular  $82 \times 69 - 82 - 69 = 5507$ .

Entonces la Proposición 1.6.1 nos asegura que la ecuación NO tiene solución con coeficientes enteros positivos.

**Ejercicio 2.** Sea  $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$  con  $p_i$  primos distintos y  $\alpha_i \in \mathbb{Z}^+$ .

Demostrar que  $n$  es un cuadrado perfecto si y solo si el número de divisores positivos de  $n$  es impar.

Solución:

*Directo:*

Si  $n$  es cuadrado perfecto entonces  $n = m^2$ , con  $m = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$ , por lo tanto  $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} = m^2 = (p_1^{\beta_1})^2 (p_2^{\beta_2})^2 \cdots (p_k^{\beta_k})^2 = p_1^{2\beta_1} p_2^{2\beta_2} \cdots p_k^{2\beta_k}$ . Entonces  $\alpha_i = 2\beta_i$ , para todo  $i = 1, 2, \dots, k$ . Luego

el  $\text{Div}_+(n) = (\alpha_1 + 1) \times (\alpha_2 + 1) \times \dots \times (\alpha_k + 1) = (2\beta_1 + 1) \times (2\beta_2 + 1) \times \dots \times (2\beta_k + 1)$ . O sea que  $\text{Div}_+(n)$  es impar.

*Recíproco:*

Si  $\text{Div}_+(n)$  es impar, como  $\text{Div}_+(n) = (\alpha_1 + 1) \times (\alpha_2 + 1) \times \dots \times (\alpha_k + 1)$ , entonces  $\alpha_i + 1$  es impar para todo  $i = 1, 2, \dots, k$ . O sea que  $\alpha_i$  es par para todo  $i = 1, 2, \dots, k$ . Por lo tanto  $\alpha_i = 2 \times \beta_i$ , para todo  $i = 1, 2, \dots, k$ . O sea que:  $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k} = (p_1^{\beta_1})^2 (p_2^{\beta_2})^2 \dots (p_k^{\beta_k})^2$ . Luego, tomando  $m = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$ , se tiene que  $n = m^2$ , es un cuadrado perfecto.

**Universidad de la República - Facultad de Ingeniería - IMERL: Matemática  
Discreta 2**

PRIMER PARCIAL - 5 DE MAYO DE 2016. DURACIÓN: 3 HORAS

**Ejercicio 1.**

- a. Calcular el inverso de 5 módulo 121.

**Solución:** Es fácil ver que  $121 - 5 \cdot 24 = 1$  (si no me doy cuenta, uso el Algoritmo de Euclides Extendido). Entonces el inverso de 5 módulo 121 es  $-24 \equiv 97 \pmod{121}$ .

- b. Calcular el inverso de  $5^4$  módulo 121.

**Solución:** Usando la parte anterior, el inverso de  $5^4$  es  $97^4$  módulo 121. Calculamos  $97^2 \equiv 92 \pmod{121}$  y  $92^2 \equiv 115 \pmod{121}$ . Entonces el inverso de  $5^4$  módulo 121 es 115.

Verificación:  $5^4 \equiv 125 \cdot 5 \equiv 4 \cdot 5 \equiv 20 \pmod{121}$  y  $20 \cdot 115 = 2300 = 19 \cdot 121 + 1$ .

- c. Calcular  $15^{773} \pmod{121}$ .

**Solución:** Como  $121 = 11^2$ , tenemos  $\varphi(121) = 11 \cdot 10 = 110$ . Como 15 es coprimo con 121, podemos usar el Teorema de Euler, obteniendo  $15^{773} \equiv 15^3 \pmod{121}$ . Ahora calculamos  $15^2 \equiv 104 \pmod{121}$  y  $104 \cdot 15 \equiv 108 \pmod{121}$ . Concluimos que  $15^{773} \equiv 108 \pmod{121}$ .

- d. Calcular  $15^{773} \pmod{5^4 \cdot 121}$

**Solución:** Usando el Teorema Chino, tenemos:

$$x \equiv 15^{773} \pmod{5^4 \cdot 121} \iff \begin{cases} x \equiv 15^{773} \pmod{5^4} \\ x \equiv 15^{773} \pmod{121} \end{cases}$$

Para resolver la primera congruencia, observamos que  $15^{773}$  es divisible por  $5^4$ , entonces  $x \equiv 0 \pmod{5^4}$ . La segunda congruencia, por la parte (c), es  $x \equiv 108 \pmod{121}$ . Ahora volvemos a usar el Teorema Chino. Queremos un entero  $x$  de la forma  $5^4 k$  que además sea congruente con 108 módulo 121. Planteamos  $5^4 k \equiv 108 \pmod{121}$ , y encontramos  $k$  usando el inverso calculado en (b):  $k \equiv 115 \cdot 108 \equiv 78 \pmod{121}$ . Concluimos que

$$\begin{cases} x \equiv 0 \pmod{5^4} \\ x \equiv 108 \pmod{121} \end{cases} \iff x \equiv 5^4 \cdot 78 \pmod{5^4 \cdot 121}$$

Entonces la solución es  $x \equiv 5^4 \cdot 78 \pmod{5^4 \cdot 121}$ .

**Ejercicio 2.** Dado el sistema

$$\begin{cases} x \equiv 31 \pmod{56} \\ x \equiv 53 \pmod{105} \end{cases},$$

investigar si tiene solución, y en caso de que tenga encontrar todas sus soluciones.

**Solución:** Observemos que 56 y 105 no son coprimos. En efecto, como ambos son divisibles entre 7, podemos mirar las dos congruencias módulo 7. La primera congruencia implica que  $x \equiv 31 \equiv 3 \pmod{7}$  y la segunda implica que  $x \equiv 53 \equiv 4 \pmod{7}$ . Como estas dos afirmaciones son contradictorias, concluimos que el sistema en cuestión no tiene ninguna solución.

**Ejercicio 3.**

- a. Probar que todo entero  $n > 1$  es producto de primos, sin utilizar el Teorema Fundamental de la Aritmética.

**Solución:** Por inducción completa (fuerte), podemos suponer que todo entero  $m$  con  $1 < m < n$  es producto de primos. Ahora consideramos dos casos:

- Si  $n$  es primo, entonces  $n$  es producto de un primo (él mismo).
- Si  $n$  no es primo, entonces  $n = ab$  con  $1 < a < n$  y  $1 < b < n$ . Por la hipótesis inductiva,  $a$  es producto de primos y  $b$  también. Pero entonces  $ab$  es producto de primos.

- b. Probar que si  $p > 2$  primo entonces es de la forma  $4k + 1$  o  $4k - 1$  con  $k$  entero.

**Solución:** Por el Teorema de División Entera, sabemos que  $p = 4q + r$  con  $q$  entero y  $r \in \{0, 1, 2, 3\}$ . Como  $p$  es impar, no puede ser  $r = 0$  o  $r = 2$ . En el caso en que  $r = 1$ , tenemos  $p = 4k + 1$  (donde  $k = q$ ). En el caso en que  $r = 3$ , tenemos  $p = 4k - 1$  (donde  $k = q + 1$ ).

- c. Probar que si un entero  $n > 1$  es de la forma  $4k - 1$ , entonces hay algún primo de la forma  $4k - 1$  que lo divide.

**Solución:** Por la parte (a)  $n$  es un producto de primos. Si 2 aparece en el producto,  $n$  sería par, contradicción. Si todos los primos que aparecen en el producto fueran de la forma  $4k + 1$ , entonces  $n$  sería también de la forma  $4k + 1$ , contradicción. Entonces en la factorización de  $n$  debe aparecer al menos un primo de la forma  $4k - 1$ .

- d. Probar que existen infinitos primos de la forma  $4k - 1$ .

**Solución:** Supongamos que los primos de la forma  $4k - 1$  son una cantidad finita, digamos que son  $p_1, p_2, \dots, p_t$ . Consideramos

$$n = 4 \cdot p_1 \cdot p_2 \cdot \dots \cdot p_t - 1,$$

que es de la forma  $4k - 1$ . Por la parte (c) hay algún primo  $q$  de la forma  $4k - 1$  que divide a  $n$ . Entonces debería ser  $q = p_i$  para algún  $i$ , luego  $p_i \mid n$  y  $p_i \mid 4p_1 \cdot p_2 \cdot \dots \cdot p_t$ , entonces  $p_i \mid 1$ , contradicción.



**Ejercicio 4.** Sean  $a \in \mathbb{Z}$  y  $n \in \mathbb{N}$  tales que  $\text{mcd}(a, n) = 1$ . Definimos los conjuntos

$$A = \{0 \leq i < n\},$$

$$B = \{0 \leq i < n : \text{mcd}(i, n) = 1\}.$$

Definimos  $f_a : A \rightarrow A$  de la siguiente manera

$$f_a(i) = a \cdot i \text{ mód } n,$$

es decir  $f_a(i)$  es el resto de la división entera de  $a \cdot i$  entre  $n$ .

- a. Probar que si  $i \in B$  entonces  $f_a(i) \in B$ .

**Solución:** Por hipótesis  $a$  es invertible módulo  $n$ . Si  $i \in B$  entonces  $i$  es invertible módulo  $n$ . Pero entonces  $a \cdot i$  también es invertible (su inverso es el producto de los inversos de  $a$  y de  $i$ ), es decir que  $f_a(i) = a \cdot i \in B$ .

- b. Probar que  $f_a$  define una biyección de  $B$  con  $B$ .

**Solución:** Denotemos  $b$  al inverso de  $a$  módulo  $n$ . Entonces la función  $f_b : B \rightarrow B$  es la inversa de  $f_a$  ya que  $f_b(f_a(i)) = f_b(a \cdot i) = b \cdot a \cdot i \equiv i \pmod{n}$ , y de la misma manera  $f_a(f_b(i)) = f_a(b \cdot i) = a \cdot b \cdot i \equiv i \pmod{n}$ . Entonces  $f_a$  es biyectiva.

- c. Probar que  $a^{\#B} \equiv 1 \pmod{n}$ .

**Solución:** Consideramos  $P \equiv \prod_{i \in B} i \pmod{n}$ . Como  $f_a$  es una biyección, entonces también  $P \equiv \prod_{i \in B} f_a(i) \pmod{n}$ , ya que la función  $f_a$  solamente cambia el orden de los factores. Entonces:

$$P \equiv \prod_{i \in B} f_a(i) \equiv \prod_{i \in B} a \cdot i \equiv a^{\#B} \prod_{i \in B} i \equiv a^{\#B} P \pmod{n}.$$

Como  $P$  es producto de invertibles, debe ser invertible y entonces podemos cancelarlo en la congruencia anterior, obteniendo así  $1 \equiv a^{\#B} \pmod{n}$ .

**Primer prueba - soluciones**

**Ejercicio 1.** Una tienda de cotillón vende chifles en bolsas de 46 unidades y bolsas de 26 unidades.

¿Cuántas bolsas de cada tipo tenemos que comprar si queremos comprar 600 chifles?

Mostrar el procedimiento para llegar a su respuesta.

Si  $x$  denota a la cantidad de bolsas de 46 unidades e  $y$  la cantidad de bolsas de 26 unidades que se comprarán, entonces necesitamos que

$$46x + 26y = 600$$

con las condiciones que  $0 \leq x, y$ .

Para simplificar, dividimos la ecuación entre 2 y nos queda:

$$23x + 13y = 300. \tag{1}$$

Como  $\text{mcd}(23, 13) = 1$  sabemos que esta ecuación diofántica tiene solución y además con el Algoritmo de Euclides Extendido, sabemos también que

$$23(4) + 13(-7) = 1.$$

Multiplicando por 300 obtenemos que

$$23(1200) + 13(-2100) = 300$$

y por lo tanto  $(x_0, y_0) = (1200, -2100)$  es una solución particular de la ecuación original. Por el Teorema de soluciones de ecuaciones diofánticas tenemos entonces que todas las soluciones de la ecuación son:

$$x = 1200 - 13k, \quad y = -2100 + 23k, \quad k \in \mathbb{Z}.$$

Para que se cumpla la condición  $0 \leq x$ , necesitamos  $k \in \mathbb{Z}$  tal que  $0 \leq 1200 - 13k$ ; es decir  $13k \leq 1200$ . Por lo tanto  $k \leq \frac{1200}{13} \sim 92,3$ . Por lo que (al ser  $k$  entero)  $k \leq 92$ .

Para que se cumpla la condición  $y \geq 0$ , necesitamos  $k \in \mathbb{Z}$  tal que  $-2100 + 23k \geq 0$ ; es decir  $23k \geq 2100$ . Por lo tanto  $k \geq \frac{2100}{23} \sim 91,3$ . Por lo que (como  $k \in \mathbb{Z}$ )  $k \geq 92$ .

De las dos condiciones resulta que la única solución al problema es tomando  $k = 92$ . Por lo tanto hay que comprar  $x = 1200 - 13(92) = 4$  bolsas de 46 unidades e  $y = -2100 + 23(92) = 16$  bolsas de 26 unidades.

**Ejercicio 2.** Para cada uno de los casos, determinar si existen naturales  $a$  y  $b$  que cumplan las siguientes ecuaciones:

1.  $27a^2 = 16b^4$

2.  $50a^3 = 27b^2$

Escribimos las descomposiciones factoriales de  $a$  y  $b$ :

$$a = \prod_{p \text{ primo}} p^{a_p}, b = \prod_{p \text{ primo}} p^{b_p}$$

(donde  $a_p, b_p \in \mathbb{N}$  y sólo una catidad finita de  $a_p$  y  $b_p$  son no nulos).

1. Tenemos que  $27a^2 = 16b^4$  si y sólo si

$$27 \left( \prod_{p \text{ primo}} p^{a_p} \right)^2 = 16 \left( \prod_{p \text{ primo}} p^{b_p} \right)^4,$$

si y sólo si

$$3^3 \prod_{p \text{ primo}} p^{2a_p} = 2^4 \prod_{p \text{ primo}} p^{4b_p}$$

Entonces tenemos que se debe cumplir que

$$2^{2a_2} 3^{3+2a_3} 5^{2a_5} \dots = 2^{4+4b_2} 3^{4b_3} 5^{4b_5} \dots$$

Por unicidad de la descomposición factorial, el exponente de cada primo en la expresión de la derecha, debe ser igual al exponente en la expresión de la izquierda. Por lo tanto, en particular, se debería cumplir que  $3 + 2a_3 = 4b_3$ , lo cual es imposible pues  $3 + 2a_3$  es impar y  $4b_3$  es par. Por lo tanto, no existen  $a, b$  que cumplan la condición.

2. De forma similar, usando que  $50 = 2 \times 5^2$  tenemos que  $50a^3 = 27b^2$  si y sólo si

$$2 \times 5^2 \prod_{p \text{ primo}} p^{3a_p} = 3^3 \prod_{p \text{ primo}} p^{2b_p}.$$

Es decir, si y sólo si

$$2^{1+3a_2} 3^{3a_3} 5^{2+3a_5} 7^{3a_7} \dots = 2^{2b_2} 3^{3+2b_3} 5^{2b_5} 7^{2a_7} \dots$$

Por unicidad de la descomposición factorial, ésto sucede si y sólo si

$$\begin{aligned} 1 + 3a_2 &= 2b_2 \\ 3a_3 &= 3 + 2b_3 \\ 2 + 3a_5 &= 2b_5 \\ 3a_p &= 2b_p, \forall p \neq 2, 3, 5 \end{aligned}$$

- La condición  $1 + 3a_2 = 2b_2$  se cumple por ejemplo tomado  $a_2 = 1$  y  $b_2 = 2$
- La condición  $3a_3 = 3 + 2b_3$  se cumple por ejemplo tomando  $a_3 = 1$  y  $b_3 = 0$ ,
- La condición  $2 + 3a_5 = 2b_5$  se cumple por ejemplo tomando  $a_5 = 0$  y  $b_5 = 1$ ,
- La condición  $3a_p = 2b_p$  para  $p \neq 2, 3, 5$ , se cumple por ejemplo tomando  $a_p = b_p = 0$ .

Por lo tanto  $a = 2^1 3^1 5^0 = 6$  y  $b = 2^2 3^0 5^1 = 20$  cumplen la condición que  $50a^3 = 27b^2$ .

Observación: si bien no pedíamos hallar todas las soluciones, notar que

- La condición  $1 + 3a_2 = 2b_2$  implica que  $a_2$  es impar; es decir  $a_2 = 2c_2 + 1$  para algún  $c_2 \in \mathbb{N}$ ; y luego  $2b_2 = 1 + 3(2c_2 + 1) = 6c_2 + 4$  y entonces  $b_2 = 3c_2 + 2$ .
- La condición  $3a_3 = 3 + 2b_3$  implica que  $2b_3 = 3a_3 - 3 = 3(a_3 - 1)$ . Por lo tanto  $3 \mid 2b_3$ , y como  $\text{mcd}(2, 3) = 1$ , por el Lema de Euclides tenemos que  $3 \mid b_3$ ; por lo tanto,  $b_3 = 3c_3$  para algún  $c_3 \in \mathbb{N}$ . Y despejando  $a_3$  obtenemos que  $a_3 = 1 + 2c_3$ .
- La condición  $2 + 3a_5 = 2b_5$  implica que  $3a_5 = 2b_5 - 2 = 2(b_5 - 1)$  y por lo tanto  $2 \mid 3a_5$  y nuevamente por el Lema de Euclides tenemos que se  $2 \mid a_5$ . Entonces  $a_5 = 2c_5$  para algún  $c_5 \in \mathbb{N}$ . Y despejando  $b_5$  obtenemos que  $b_5 = 1 + 3c_5$ .
- La condición  $3a_p = 2b_p$  para  $p \neq 2, 3, 5$ , implica que (por el Lema de Euclides nuevamente)  $2 \mid a_p$ , es decir que  $a_p = 2c_p$  para algún  $c_p \in \mathbb{N}$ . Y despejando  $b_p$  obtenemos que  $b_p = 3c_p$ .

Es decir que ara obtener todas las soluciones basta con conciderar para cada primo  $p$ ,  $c_p \in \mathbb{N}$ , con sólo una cantidad finita no nulos; y luego

$$\begin{aligned} a &= 2^{1+2c_2} 3^{1+2c_3} 5^{2c_5} \prod_{\substack{2,3,5 \neq p \\ \text{primo}}} p^{2c_p} \\ b &= 2^{2+3c_2} 3^{3c_3} 5^{1+3c_5} \prod_{\substack{2,3,5 \neq p \\ \text{primo}}} p^{3c_p} \end{aligned}$$

Y si llamamos  $c = \prod_{p \text{ primo}} p^{c_p}$  (es decir  $c$  es cualquier natural mayor que 1), obtenemos que todas las soluciones son  $a = 2^1 3^1 c^2 = 6c^2$  y  $b = 2^2 5^1 c^3 = 20c^3$ .

**Universidad de la República - Facultad de Ingeniería - IMERL: Matemática Discreta 2**

PRIMER PARCIAL - 4 DE MAYO DE 2015. DURACIÓN: 3 HORAS

**Ejercicio 1.** Sea  $0 \leq n < 99$  tal que  $n \equiv 5^{2579} \pmod{99}$ . Indicar cuál de las opciones es correcta:

- A.  $n = 56$ .                      B.  $n = 20$ .                      C.  $n = 86$ .                      D.  $n = 5$ .

Como 5 y 99 son coprimos podemos aplicar el teorema de Euler. Como  $99 = 3^2 \cdot 11$  entonces  $\varphi(99) = 2 \cdot 3 \cdot 10 = 60$ . También  $2579 \equiv -1 \pmod{60}$  y aplicando el teorema de Euler

$$5^{2579} \equiv 5^{-1} \pmod{99}.$$

Aplicando el Algoritmo Extendido de Euclides, el inverso de 5 módulo 99 es 20. Por lo tanto la solución es **20**.

**Ejercicio 2.** Sea  $0 \leq m < 297$  tal que  $m \equiv 60^{181} \pmod{297}$ . Indicar cuál de las opciones es correcta:

- A.  $m = 60$ .                      B.  $m = 27$ .                      C.  $m = 135$ .                      D.  $m = 81$ .

Como  $60 = 2^2 \cdot 3 \cdot 5$  no es coprimo con  $297 = 3^3 \cdot 11$  no podemos aplicar el teorema de Euler. Aplicando el Teorema Chino del Resto obtenemos

$$x \equiv 60^{181} \pmod{297} \Leftrightarrow \begin{cases} x \equiv 60^{181} \pmod{3^3} \\ x \equiv 60^{181} \pmod{11} \end{cases} \Leftrightarrow \begin{cases} x \equiv 3^{181} \cdot 20^{181} \pmod{3^3} \\ x \equiv 60^{181} \pmod{11} \end{cases}.$$

Ahora como  $3^3 \mid 3^{181}$  entonces  $60^{181} \equiv 0 \pmod{3^3}$ . Por otro lado  $\varphi(11) = 10$  y  $181 \equiv 1 \pmod{10}$ , por lo que  $60^{181} \equiv 60 \pmod{11} \equiv 5 \pmod{11}$ . Concluimos que

$$x \equiv 60^{181} \pmod{297} \Leftrightarrow \begin{cases} x \equiv 0 \pmod{3^3} \\ x \equiv 5 \pmod{11} \end{cases},$$

que tiene solución **27**.

## Segunda parte: Desarrollo

**Ejercicio 3.** Sean  $a, b, c \in \mathbb{Z}^+$ , probar que:

- a.  $\text{mcd}(a, b) = \min \{s > 0 : s = ax + by \text{ para algunos } x, y \in \mathbb{Z}\}.$

Ver notas de teórico.

- b. Si  $\text{mcd}(a, b) = 1$  y  $a \mid bc$  entonces  $a \mid c$ .

Ver notas de teórico.

(Cualquier resultado que utilicen en esta parte tienen que demostrarlo).

**Ejercicio 4.** Dado el sistema

$$\begin{cases} x \equiv 8 & (\text{mód } 56) \\ x \equiv 1 & (\text{mód } 21) \\ x \equiv 4 & (\text{mód } 36) \\ x \equiv 8 & (\text{mód } 49) \end{cases},$$

investigar si tiene solución, y en caso que tenga encontrar todas sus soluciones.

Como  $56 = 2^3 \cdot 7$ ,  $21 = 3 \cdot 7$ ,  $36 = 2^2 \cdot 3^2$  y  $49 = 7^2$ , entonces

$$x \equiv 8 \pmod{56} \Leftrightarrow \begin{cases} x \equiv 8 & (\text{mód } 8) \\ x \equiv 8 & (\text{mód } 7) \end{cases} \Leftrightarrow \begin{cases} x \equiv 0 & (\text{mód } 8) \\ x \equiv 1 & (\text{mód } 7) \end{cases}, \quad (1)$$

$$x \equiv 1 \pmod{21} \Leftrightarrow \begin{cases} x \equiv 1 & (\text{mód } 3) \\ x \equiv 1 & (\text{mód } 7) \end{cases} \Leftrightarrow \begin{cases} x \equiv 1 & (\text{mód } 3) \\ x \equiv 1 & (\text{mód } 7) \end{cases}, \quad (2)$$

$$x \equiv 4 \pmod{36} \Leftrightarrow \begin{cases} x \equiv 4 & (\text{mód } 4) \\ x \equiv 4 & (\text{mód } 9) \end{cases} \Leftrightarrow \begin{cases} x \equiv 0 & (\text{mód } 4) \\ x \equiv 4 & (\text{mód } 9) \end{cases}. \quad (3)$$

Como  $x \equiv 0 \pmod{8}$  implica  $x \equiv 0 \pmod{4}$ ,  $x \equiv 4 \pmod{9}$  implica  $x \equiv 4 \pmod{9}$  y  $x \equiv 8 \pmod{49}$  implica  $x \equiv 1 \pmod{7}$ , entonces el sistema original es **equivalente** a

$$\begin{cases} x \equiv 0 & (\text{mód } 8) \\ x \equiv 4 & (\text{mód } 9) \\ x \equiv 8 & (\text{mód } 49) \end{cases}$$

que tiene solución **400 módulo  $8 \cdot 9 \cdot 49 = 3528$** .

**Ejercicio 5.**

- a. Sea  $p$  primo, probar que si  $x^2 \equiv 1 \pmod{p}$  entonces  $x \equiv 1 \pmod{p}$  o  $x \equiv -1 \pmod{p}$ .

Si  $x^2 \equiv 1 \pmod{p}$  entonces  $0 \equiv (x^2 - 1) \pmod{p} \equiv (x - 1)(x + 1) \pmod{p}$  y  $p \mid (x - 1)(x + 1)$ .

Ahora, como  $p$  es primo  $p \mid (x - 1)$  o  $p \mid (x + 1)$ , por lo cual

$$x \equiv 1 \pmod{p} \text{ o } x \equiv -1 \pmod{p}.$$

Observar que ambas posibilidades son ciertas si y solo si  $p = 2$  ya que en ese caso  $1 \equiv -1 \pmod{p}$  que implica  $p \mid 2$ .

- b. Sea  $n = pqr$  con  $p, q, r$  primos distintos. Probar que hay a lo sumo 8 soluciones módulo  $n$  a la ecuación  $x^2 \equiv 1 \pmod{n}$ .

Si  $x^2 \equiv 1 \pmod{pqr}$  entonces  $x^2 \equiv 1 \pmod{p}$ ,  $x^2 \equiv 1 \pmod{q}$  y  $x^2 \equiv 1 \pmod{r}$ . Usando la parte anterior sabemos que

$$\begin{cases} x \equiv 1 & (\text{mód } p) \\ \text{o} \\ x \equiv -1 & (\text{mód } p) \end{cases} \text{ y } \begin{cases} x \equiv 1 & (\text{mód } q) \\ \text{o} \\ x \equiv -1 & (\text{mód } q) \end{cases} \text{ y } \begin{cases} x \equiv 1 & (\text{mód } r) \\ \text{o} \\ x \equiv -1 & (\text{mód } r) \end{cases}$$

por lo que

$$\begin{aligned}
& \left\{ \begin{array}{l} x \equiv 1 \pmod{p} \\ y \equiv 1 \pmod{q} \\ x \equiv 1 \pmod{r} \end{array} \right. \text{ o } \left\{ \begin{array}{l} x \equiv 1 \pmod{p} \\ y \equiv -1 \pmod{q} \\ x \equiv 1 \pmod{r} \end{array} \right. \text{ o } \left\{ \begin{array}{l} x \equiv 1 \pmod{p} \\ y \equiv -1 \pmod{q} \\ x \equiv -1 \pmod{r} \end{array} \right. \\
& \left\{ \begin{array}{l} x \equiv 1 \pmod{p} \\ y \equiv 1 \pmod{q} \\ x \equiv -1 \pmod{r} \end{array} \right. \text{ o } \left\{ \begin{array}{l} x \equiv -1 \pmod{p} \\ y \equiv 1 \pmod{q} \\ x \equiv 1 \pmod{r} \end{array} \right. \text{ o } \left\{ \begin{array}{l} x \equiv -1 \pmod{p} \\ y \equiv -1 \pmod{q} \\ x \equiv 1 \pmod{r} \end{array} \right. \text{ o } \\
& \left\{ \begin{array}{l} x \equiv -1 \pmod{p} \\ y \equiv 1 \pmod{q} \\ x \equiv -1 \pmod{r} \end{array} \right. \text{ o } \left\{ \begin{array}{l} x \equiv -1 \pmod{p} \\ y \equiv -1 \pmod{q} \\ x \equiv -1 \pmod{r} \end{array} \right. ,
\end{aligned}$$

que son las 8 opciones posibles.

**Primer parcial - soluciones**

Para los ejercicios 1, 5 y 6 ver las notas del teórico.

**Ejercicio 2.**

a) **Hallar el resto de dividir  $11^{1604}$  entre 1200.**

Como  $\varphi(1200) = \varphi(2^4 \cdot 3 \cdot 5^2) = (2^4 - 2^3)2(5^2 - 5) = 320$ , se tiene que:

$$11^{1604} = 11^{320 \cdot 5 + 4} = (11^{\varphi(1200)^5}) \cdot 11^4 \equiv 11^4 = 121^2 = 14641 = 12000 + 1200 \cdot 2 + 241 \equiv 241 \pmod{1200},$$

luego el resto buscado es 241.

b) **Hallar el resto de dividir  $7^{319}$  entre 1200.**

Por la parte a) sabemos que:  $7^{319} = 7^{320-1} = 7^{\varphi(1200)} \cdot 7^{-1} \equiv 7^{-1} \pmod{1200}$ , luego habría que hallar el inverso de 7 módulo 1200.

Para resolver la ecuación  $7x \equiv 1 \pmod{1200}$  consideremos la ecuación diofántica:  $7x - 1200y = 1$ . Tenemos:

$$\begin{array}{r|rr} (1200) & 1 & 0 \\ (7) & 0 & 1 \\ \hline 1200 = 7 \cdot 171 + 3 & 1 & -171 \\ 7 = 3 \cdot 2 + 1 & -2 & 343 \end{array}$$

por lo que  $1 = -2 \cdot 1200 + 343 \cdot 7$  y  $x \equiv 343 \pmod{1200}$ .

**Ejercicio 3.**

Una compañía compró cierto número de reliquias falsas a 46 pesos cada una y vendió algunas de ellas a 100 pesos cada una. Si la cantidad comprada originalmente es mayor que 400 pero menor que 500 y la compañía obtuvo una ganancia de 1000 pesos, ¿cuántas reliquias no se vendieron?

Si  $y$  denota a la cantidad de reliquias compradas y  $x$  la de vendidas, la ganancia se puede expresar como la resta  $100x - 46y$ . Luego tenemos que resolver la ecuación diofántica

$$100x - 46y = 1000$$

con la condición de que  $400 < y < 500$ , y la respuesta, o sea la cantidad de reliquias que no se vendieron, será  $y - x$ .

Para simplificar, dividimos la ecuación entre 2 y nos queda:

$$50x - 23y = 500. \tag{1}$$

Una solución evidente es  $x_0 = 10$  e  $y = 0$ , luego la solución general tiene la forma:  $x = 10 + 23t$  e  $y = 50t$ , donde  $t$  es un número entero, ya que  $\text{mcd}(50, 23) = 1$ . La condición  $400 < y < 500$  entonces implica  $400 < 50t < 500$ . Dividiendo entre 50 esto se reduce a  $8 < t < 10$ , de donde  $t = 9$ . Entonces,  $x = 10 + 23t = 217$  e  $y = 50t = 450$  y quedan:  $y - x = 450 - 217 = 233$  reliquias que no se vendieron.



#### Ejercicio 4.

a) Hallar todas las soluciones módulo 15 de la ecuación:

$$6x \equiv 9 \pmod{15}.$$

Como  $\text{mcd}(6, 15) = 3$  la ecuación tiene una única solución módulo  $\frac{15}{3} = 5$  y va a tener 3 soluciones módulo 15.

Dividiendo entre 3 obtenemos:

$$2x \equiv 3 \pmod{5}.$$

De aquí:

$$2x \equiv 3 + 5 \pmod{5}$$

luego  $x \equiv 4 \pmod{5}$  y  $x \equiv 4; 9; 14 \pmod{15}$ .

b) Investigar si el siguiente sistema tiene solución:

$$\begin{cases} x \equiv 14 \pmod{36} \\ x \equiv 23 \pmod{27} \\ x \equiv 10 \pmod{12} \end{cases}$$

Basta con darse cuenta que la segunda ecuación implica:  $x \equiv 23 \pmod{3}$  (ya que  $3|27$ ) lo que se reduce a  $x \equiv 2 \pmod{3}$ , mientras que la tercera implica  $x \equiv 10 \pmod{3}$  (ya que  $3|12$ ) lo que se reduce a  $x \equiv 1 \pmod{3}$ . Esto es imposible, ya que  $x$  no puede ser simultáneamente congruente a 2 y a 1 módulo 3, y el sistema no tiene solución.

c) Resolver el sistema:

$$\begin{cases} 5x \equiv 11 \pmod{12} \\ 2x \equiv 5 \pmod{9} \\ x \equiv 9 \pmod{10} \end{cases}$$

Primero nos damos cuenta de que todas las tres ecuaciones tienen única solución con respecto a sus módulos respectivos, ya que  $\text{mcd}(5, 12) = 1 = \text{mcd}(2, 9)$ .

En la primera ecuación tenemos:  $5x \equiv 11 \equiv 11 + 2 \cdot 12 = 35 \pmod{12}$ , luego  $x \equiv 7 \pmod{12}$ , ya que  $\text{mcd}(5, 12) = 1$ .

En la segunda tenemos:  $2x \equiv 5 \equiv 5 + 9 = 14 \pmod{9}$ , luego  $x \equiv 7 \pmod{9}$ , ya que  $\text{mcd}(2, 9) = 1$ . Ahora nos queda resolver el sistema:

$$\begin{cases} x \equiv 7 \pmod{12} \\ x \equiv 7 \pmod{9} \\ x \equiv 9 \pmod{10} \end{cases}$$

La primera ecuación es equivalente a:  $x \equiv 7 \pmod{3}$  y  $x \equiv 7 \equiv 3 \pmod{4}$  ( $\Rightarrow x \equiv 1 \pmod{2}$ ).

La segunda implica:  $x \equiv 7 \pmod{3}$ .

La tercera es equivalente a:  $x \equiv 9 \equiv 1 \pmod{2}$  y  $x \equiv 9 \equiv 4 \pmod{5}$ .

Entonces, es suficiente resolver el siguiente sistema:

$$\begin{cases} x \equiv 3 \pmod{4} \\ x \equiv 7 \pmod{9} \\ x \equiv 4 \pmod{5} \end{cases}$$

Resolviendo las primeras dos ecuaciones tenemos:

$$x = 3 + 4k \equiv 7 \pmod{9}$$

luego

$$4k \equiv 4 \pmod{9} \Rightarrow k \equiv 1 \pmod{9}$$

ya que  $\text{mcd}(4, 9) = 1$ . Entonces,  $k = 1 + 9t$  y  $x = 3 + 4k = 3 + 4(1 + 9t) = 7 + 36t$ . Agregando la tercera ecuación tenemos:

$$7 + 36t \equiv 4 \pmod{5} \Leftrightarrow 2 + t \equiv 4 \pmod{5}.$$

Entonces,  $t \equiv 2 \pmod{5} \Rightarrow t = 2 + 5s \Rightarrow x = 7 + 36t = 7 + 36(2 + 5s) = 79 + 180s$ , luego  $x \equiv 79 \pmod{180}$ .

**Ejercicio 1) Sea  $S_a$  el sistema de congruencias**

$$S_a \begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 4 \pmod{7} \\ x \equiv 5 \pmod{11} \\ x \equiv a \pmod{21} \end{cases}$$

**a) Hallar el mínimo  $a \in \mathbb{N}$  para que el sistema  $S_a$  tenga solución.**

Por el teorema chino de los restos,  $S_a$  es equivalente al sistema

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 4 \pmod{7} \\ x \equiv 5 \pmod{11} \\ x \equiv a \pmod{3} \\ x \equiv a \pmod{7} \end{cases}$$

Y dicho sistema tiene solución si y sólo si el sistema

$$\begin{cases} a \equiv 2 \pmod{3} \\ a \equiv 4 \pmod{7} \end{cases}$$

tiene solución. Como  $a = 3 \cdot 3 + 2 = 7 + 4 = 11$  es solución de

$$\begin{cases} a \equiv 2 \pmod{3} \\ a \equiv 4 \pmod{7} \end{cases}$$

Más aún por el teorema chino de los restos, cualquier otro  $a$  que sea solución es congruente con 11 módulo  $3 \cdot 7 = 21$ . O sea que 11 es el menor natural tal que el sistema  $S_a$  tenga solución.

**b) Determinar la solución del sistema para el  $a$  hallado en la parte anterior y probar que la solución es única módulo 231.**

El sistema  $S_a$  con  $a = 11$  queda

$$S_{11} \begin{cases} x \equiv 2 & (\text{mod } 3) \\ x \equiv 4 & (\text{mod } 7) \\ x \equiv 5 & (\text{mod } 11) \\ x \equiv 11 & (\text{mod } 21) \end{cases}$$

o lo que es lo mismo

$$\begin{cases} x \equiv 2 & (\text{mod } 3) \\ x \equiv 4 & (\text{mod } 7) \\ x \equiv 5 & (\text{mod } 11) \end{cases}$$

El sistema

$$\begin{cases} x \equiv 2 & (\text{mod } 3) \\ x \equiv 4 & (\text{mod } 7) \end{cases}$$

ya fue resuelto en la parte anterior y se concluyó  $x \equiv 11 \pmod{21}$ .

Luego, resolver  $S_{11}$  es resolver

$$\begin{cases} x \equiv 5 & (\text{mod } 11) \\ x \equiv 11 & (\text{mod } 21) \end{cases}$$

Como  $x = 6 \cdot 21 + 11 = 12 \cdot 11 + 5 = 137$  es solución de  $S_{11}$ . Luego cualquier otra solución de  $S_{11}$  es congruente con 137 módulo  $3 \cdot 7 \cdot 11 = 231$ .

### Ejercicio 2)

**a) Dado  $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_t^{\alpha_t}$  con  $\alpha_i \geq 1$  y  $p_i$  primos para todo  $i = 1, \dots, t$ , determinar el número de divisores y demostrar el resultado.**

Como  $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_t^{\alpha_t}$  entonces todos los divisores de  $n$  serán de la forma  $p_1^{\beta_1} p_2^{\beta_2} \dots p_t^{\beta_t}$  con  $0 \leq \beta_i \leq \alpha_i$  para todo  $i$ . Luego  $n$  tiene tantos divisores como  $(\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_t + 1)$ .

**b) Probar que, si un número es un cubo perfecto, entonces su cantidad de divisores positivos es congruente con 1 módulo 3.**

Si un número  $n$  es un cubo perfecto, entonces  $n = a^3$  para cierto entero  $a$ . Luego, si  $a = p_1^{\alpha_1} \dots p_t^{\alpha_t}$  es la descomposición en primos de  $a$ ,  $n = p_1^{3\alpha_1} \dots p_t^{3\alpha_t}$  será la descomposición en primos de  $n$ . Pero entonces la cantidad de divisores de  $n$  es  $(3\alpha_1 + 1)(3\alpha_2 + 1) \dots (3\alpha_t + 1)$ ; y como cada uno de estos factores es congruente con 1 módulo 3, entonces su producto también lo será.

**c) ¿Es cierto el recíproco? Caso afirmativo: demostrarlo. Caso negativo: dar contraejemplo.**

Es falso: sea  $n = 2 \cdot 5 = 10$ . Luego  $n$  no es un cubo perfecto pero tiene exactamente  $4 = 3 + 1$  divisores (1, 2, 5 y 10).

**d) Se tiene un tablero de  $18 \times 20$  casillas y se ponen granos de arroz en las casillas de modo que todas tengan la misma cantidad. ¿Cuál es la menor cantidad de granos que se deben colocar en cada casilla para que la cantidad total de granos sea un cubo perfecto?**

Sea  $n$  la cantidad de granos que se ponen en cada casilla. O sea que en total hay  $18 \cdot 20 \cdot n$  granos en el tablero. Ahora, para que esta cantidad sea un cubo perfecto, es necesario (por la parte **a**) y obviamente suficiente, que todos los primos de la descomposición de  $18 \cdot 20 \cdot n$  aparezcan con exponente múltiplo de 3.

Y como  $18 \cdot 20 = 2 \cdot 3^2 \cdot 2^2 \cdot 5 = 2^3 \cdot 3^2 \cdot 5$  entonces el menor  $n$  posible es  $n = 3 \cdot 5^2$ .

### Ejercicio 3)

Sea  $\phi$  la función de Euler.

**a) Demostrar que  $\phi(p^n) = p^{n-1}(p-1)$  para  $p$  primo y  $n \geq 1$ .**

$$\phi(p^n) = \#\{0 \leq a \leq p^n : \text{mcd}(a, p^n) = 1\} = \#(\{0 \leq a \leq p^n\} - \{0 \leq a \leq p^n : \text{mcd}(a, p^n) \neq 1\}) = p^n - \#\{0 \leq a \leq p^n : \text{mcd}(a, p^n) \neq 1\}.$$

Como  $p$  es primo, entonces  $\text{mcd}(a, p^n) \neq 1$  si y solo si  $p|a$ . Luego  $\{0 \leq a \leq p^n : \text{mcd}(a, p^n) \neq 1\} = \{0 \leq a \leq p^n : p|a\}$  y entonces  $\phi(p^n) = p^n - p^{n-1}$ .

**b) Sean  $m = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3}$  y  $n = p_2^{\beta_2} p_3^{\beta_3} p_4^{\beta_4}$  donde los  $p_i$  son primos para**

$i = 1, 2, 3, 4$ ,  $\alpha_i \geq 1$  para  $i = 1, 2, 3$ ,  $\beta_i \geq 1$  para  $i = 2, 3, 4$ ,  $\alpha_2 \leq \beta_2$  y  $\beta_3 < \alpha_3$ .

**b)1) Hallar  $d = \text{mcd}(m, n)$ .**

El máximo común divisor de dos números es el producto de todos los primos comunes con el menor exponente. Luego como  $p_1, p_2, p_3$  y  $p_4$  son primos distintos y  $\alpha_2 \leq \beta_2$ ,  $\beta_3 < \alpha_3$ ,  $\text{mcd}(n, m) = \text{mcd}(p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3}, p_2^{\beta_2} p_3^{\beta_3} p_4^{\beta_4}) = p_2^{\alpha_2} p_3^{\beta_3}$ .

**b)2) Probar que  $\phi(mn) = \frac{\phi(m)\phi(n)d}{\phi(d)}$ .**

$$\phi(n \cdot m) = p_1^{\alpha_1-1}(p_1-1)p_2^{\alpha_2+\beta_2-1}(p_2-1)p_3^{\alpha_3+\beta_3-1}(p_3-1)p_4^{\beta_4-1}(p_4-1).$$

$$\phi(n) = p_1^{\alpha_1-1}(p_1-1)p_2^{\alpha_2-1}(p_2-1)p_3^{\alpha_3-1}(p_3-1)$$

$$\phi(m) = p_2^{\beta_2-1}(p_2-1)p_3^{\beta_3-1}(p_3-1)p_4^{\beta_4-1}(p_4-1)$$

$$\phi(d) = p_2^{\alpha_2-1}(p_2-1)p_3^{\beta_3-1}(p_3-1).$$

Luego se obtiene lo querido.

**c) Calcular  $10 \cdot 17^{2306} \pmod{60 \cdot 42}$ .**

Por la parte anterior sabemos que  $\phi(60 \cdot 42) = \frac{\phi(60) \cdot \phi(42) \cdot 6}{\phi(6)} = \frac{(2^4) \cdot (2 \cdot 3) \cdot 6}{2} = 576$ . Por lo tanto como  $10 \cdot 17^{2306} = 10 \cdot 17^{4 \cdot 576 + 2}$  usando el Teorema de Euler tenemos que  $10 \cdot 17^{2306} \equiv 10 \cdot 17^2 \equiv 370 \pmod{60 \cdot 42}$ .

## PRIMER PARCIAL DE MATEMÁTICA DISCRETA 2

Nombre .....	C.I. ....	No. de prueba .....
--------------	-----------	---------------------

Duración: 3 horas y media. **Sin** material y **sin** calculadora.

Es necesario mostrar la resolución de los ejercicios y el procedimiento para llegar a la respuesta. Presentar únicamente la respuesta final carece de valor.

**Ejercicio 1.**

A. Sean  $a, b$  y  $c \in \mathbb{Z}$  tales que  $\text{mcd}(a, b) = 1$ ,  $a \mid c$  y  $b \mid c$ . Probar que  $ab \mid c$ .

**Aclaración:** si se utilizan lemas, teoremas o propiedades, éstos deberán ser enunciados, pero no es necesario demostrarlos.

B. Sean  $m_1$  y  $m_2$  dos enteros coprimos y  $a_1, a_2 \in \mathbb{Z}$ . Probar que si  $x_1$  y  $x_2$  son soluciones del sistema  $\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \end{cases}$  entonces  $x_1 \equiv x_2 \pmod{m_1 m_2}$ .

**Aclaración:** en esta parte B. se pide demostrar parte del Teorema Chino del Resto, y por lo tanto no serán válidas las respuestas que utilicen dicho teorema.

C. Hallar el menor  $x \in \mathbb{N}$  que verifica  $\begin{cases} x \equiv 1 \pmod{5} \\ x \equiv 0 \pmod{8} \\ x \equiv 1 \pmod{9} \end{cases}$ .

D. Investigar si los siguientes sistemas tienen solución, y en caso de que así sea, hallar todas las soluciones en  $\mathbb{Z}$ .

$$\begin{cases} x \equiv 16 \pmod{40} \\ x \equiv 1 \pmod{15} \\ x \equiv 10 \pmod{18} \end{cases} \quad \text{y} \quad \begin{cases} x \equiv 16 \pmod{40} \\ x \equiv 6 \pmod{15} \\ x \equiv 10 \pmod{18} \end{cases}$$

**Ejercicio 2.** Las partes de este ejercicio son independientes.

A. Probar que para todo  $n \in \mathbb{N}$ ,  $n \geq 1$ ,  $\text{mcd}(2^n + 7^n, 2^n - 7^n) = 1$ .

B. Hallar todos los  $n \in \mathbb{N}$  tales que  $\text{mcd}(n, 1260) = 70$  y  $n$  tiene 30 divisores positivos.

C. Probar que para todo  $n \in \mathbb{N}$ ,  $n \geq 1$ ,  $3^n$  divide a  $64^{3^n-1} - 1$ .

**Ejercicio 3.**

A. Sean  $a, b, c$  enteros no nulos y la ecuación  $ax + by = c$ . Probar que si  $(x_0, y_0)$  y  $(x_1, y_1)$  son soluciones enteras de la ecuación, entonces existe  $k \in \mathbb{Z}$  tal que

$$x_1 = x_0 + k \frac{b}{\text{mcd}(a, b)} \text{ y } y_1 = y_0 - k \frac{a}{\text{mcd}(a, b)}.$$

**Aclaración:** en esta parte A. se pide demostrar parte del Teorema de soluciones de una ecuación diofántica, y por lo tanto no serán válidas las respuestas que utilicen dicho teorema. Si se utiliza otro teorema, lemas o propiedades, éstos deberán ser enunciados, pero no es necesario demostrarlos.

B. Hallar todos los  $c \in \mathbb{Z}$  que son inversos de 9 módulo 1190.

C. Hallar el resto de dividir  $3^{382}$  entre 1190.

## PRIMER PARCIAL DE MATEMÁTICA DISCRETA 2

Nombre .....	C.I. ....	No. de prueba .....
--------------	-----------	---------------------

Duración: 3:30 horas. Sin material y sin calculadora.

Es necesario mostrar la resolución de los ejercicios, presentar únicamente la respuesta final carece de valor.

### Ejercicio 1. (12 puntos)

- Enuncie (y **NO** demuestre) el Teorema de Euler.
- Hallar el valor de  $x \in \{0, 1, 2, \dots, 34\}$  tal que  $x \equiv 102^{201} \pmod{35}$ .
- Hallar el resto de dividir  $30^{3998}$  entre 4001. (Observación: 4001 es primo, y no es necesario probarlo).

### Ejercicio 2. (16 puntos)

- Enuncie (y **NO** demuestre) el Teorema Chino del Resto.
- Sea  $\varphi(n)$  la cantidad de naturales coprimos con  $n$  que son menores o iguales que  $n$ . Probar que

$$\text{si } \text{mcd}(n, m) = 1 \text{ entonces } \varphi(nm) = \varphi(n)\varphi(m).$$

(Sugerencia: encontrar una biyección entre dos conjuntos, uno con cardinal  $\varphi(nm)$  y otro con cardinal  $\varphi(n)\varphi(m)$ . Cualquier propiedad de  $\varphi$  que se utilice en esta parte deberá probarse).

- Probar que si  $d, m \in \mathbb{N}$  y  $d|m$  entonces  $\varphi(dm) = d\varphi(m)$ .
- Probar que si un entero  $n > 4$  es compuesto, entonces  $n$  divide a  $(n-1)!$  (Sugerencia: discutir según si  $n$  es producto de dos coprimos o no).
- Calcular  $\varphi(n!)/\varphi((n-1)!)$  para todo  $n \geq 2$ . (Sugerencia: discutir según si  $n$  es primo o compuesto).

### Ejercicio 3. (12 puntos)

- Sea  $(G, \cdot)$  un grupo y  $x \in G$  un elemento que verifica  $x \cdot g_0 = g_0$  para algún  $g_0 \in G$ . Probar que  $x \cdot g = g$  para todo  $g \in G$ .
- Probar que en una misma columna o fila de la tabla de Cayley de un grupo no aparecen elementos repetidos.
- La tabla abajo representa la tabla de Cayley (tabla de multiplicación) de un grupo.
  - Hallar el elemento neutro del grupo.
  - Hallar el orden del elemento  $g_2$ .
  - Completar (justificando) la tabla de Cayley.

$\cdot$	$g_1$	$g_2$	$g_3$	$g_4$	$g_5$	$g_6$
$g_1$		$g_6$		$g_5$		
$g_2$		$g_1$				
$g_3$	$g_5$	$g_4$	$g_6$			
$g_4$		$g_5$		$g_6$		
$g_5$		$g_3$			$g_6$	
$g_6$						



# PRIMER PARCIAL DE MATEMÁTICA DISCRETA II

Nombre .....	C.I. ....	No. de prueba .....
--------------	-----------	---------------------

## Ejercicio 1.

- A. Hallar  $a, b \in \mathbb{N}$  tales que  $a > b$ , el resto de dividir  $a$  entre  $b$  es 7 y  $\text{mcm}(a, b) = 26 \text{ mcd}(a, b)$ .
- B. Probar que  $5^{4n+1} + 2 \cdot 4^{6n+1}$  es múltiplo de 13 para todo  $n \in \mathbb{N}$ .

## Ejercicio 2.

- A. Hallar el menor  $x \in \mathbb{N}$  que verifica 
$$\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 0 \pmod{4} \\ x \equiv 6 \pmod{7} \end{cases}$$
- B. Calcular el resto de dividir  $34^{1234}$  entre 84.

## Ejercicio 3.

- A. Sean  $a, n \in \mathbb{N}$ . Probar que si  $\text{mcd}(a, n) = 1$  entonces existe  $x \in \mathbb{Z}$  tal que  $ax \equiv 1 \pmod{n}$ .
- B. Sea  $p \in \mathbb{N}$ ,  $p \geq 2$ . Probar que  $p$  es primo si y solo si para todo  $a \in \{1, 2, \dots, p-1\}$  existe  $x \in \{1, 2, \dots, p-1\}$  tal que  $ax \equiv 1 \pmod{p}$ .
- C. Hallar  $x \in \{1, 2, \dots, 126\}$  tal que  $55x \equiv 1 \pmod{127}$ .

## Ejercicio 4.

- A. Sean  $n \in \mathbb{N}$  y  $\{r_1, r_2, \dots, r_{\varphi(n)}\}$  un sistema reducido de residuos módulo  $n$ . Probar que si  $a \in \mathbb{N}$  y  $\text{mcd}(a, n) = 1$  entonces  $\{ar_1, ar_2, \dots, ar_{\varphi(n)}\}$  es también un sistema reducido de residuos módulo  $n$ .
- B. Enunciar y demostrar el teorema de Euler.
- C. Hallar el resto de dividir  $33^{482}$  entre 35.