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

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

N° 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 $\operatorname{mcd}(a, n) = 1$ entonces a es invertible módulo n.

c. Hallar el inverso de 7 módulo 11.

d. Hallar $x \in \{0, 1, \cdots, 10\}$ tal que $x \equiv 7^{139} \pmod{11}$.

e. Hallar $x \in \{0, 1, \cdots, 15\}$ 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 $\operatorname{mcd}(a, b) = \min\{c > 0 : c = ax + by \text{ con } x, y \in \mathbb{Z}\}$.

b. Sean $a, b \in \mathbb{Z}$ tales que $\operatorname{mcd}(a, b) = 1$.

- **i**) Probar que si p es un primo divisor común de $(a + 2b)$ y ab, entonces $p = 2$.
- **ii**) Hallar $\operatorname{mcd}(a + 2b, ab)$ discutiendo según la paridad de a.

Ejercicio 3.

a. Hallar todos $a, b \in \mathbb{N}$ tales que $\operatorname{mcd}(a, b) = 12$, 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 $k = 1, \cdots, n-1$, se tiene que

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

Solución primer parcial - 27 de abril de 2017.

Ejercicio 1. Encontrar todos los $a, b \in \mathbb{N}$ tales que $a + b = 407$ y $\operatorname{mcm}(a, b) = 210 \operatorname{mcd}(a, b)$.
Solución: Sean $d = \operatorname{mcd}(a, b)$ 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 $\operatorname{mcm}(a, b) \operatorname{mcd}(a, b) = ab$, tenemos

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

Por lo tanto

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

Recordemos que $\operatorname{mcd}(a^*, b^*) = 1$ 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 $\operatorname{mcd}(a, b) \mid c$.
Solución: Sea $d = \operatorname{mcd}(a, b)$. 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

$$\begin{cases} x & \equiv & 6 \pmod{13} \\ x & \equiv & 62 \pmod{103} \end{cases}$$

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 $\operatorname{mcd}(e, \varphi(n)) = 1$. 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 $\operatorname{mcd}(x, n) = 1$.

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

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

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

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

Entonces

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

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

$$\left\{ \begin{array}{lcll} x & \equiv & a_1 & \pmod{m_1} \\ x & \equiv & a_2 & \pmod{m_2} \end{array} \right. , x \in \mathbb{Z},$$

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 $\operatorname{mcd}(m_1, m_2) = 1$, 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 $\operatorname{mcd}(m_1, m_2) = 1$ 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 $\mathrm{mcd}(82, 69) = 1$ 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 $\mathrm{mcd}(738, 621) = 9$.

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 $\mathrm{mcd}(738, 621) = 9$ 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 $i = 1, 2, ..., k$. Luego

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

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

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

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 $p_1, p_2, \ldots, p_t$. Consideramos

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

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 $p_i \mid 4p_1 \cdot p_2 \cdot \cdots \cdot p_t$, entonces $p_i \mid 1$, contradicción.

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

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

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

$$f_a(i) = a \cdot i \bmod n \,,$$

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 $f_b : B \to B$ 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 - 11 de ssetiembre de 2015. Duración: 1 hora y media

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:

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

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 $-2100 + 23k \geq$; 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

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

   Por unicidad de la descomposición factorial, el exponenete 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

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

   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 $\mathrm{mcd}(2,3) = 1$, 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 concíderar para cada primo p, $c_p \in \mathbb{N}$, con sólo una cantidad finita no nulos; y luego

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

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 $b = 2^2 5^1 c^3 = 20c^3$.

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

$$x \equiv 60^{181} \pmod{297} \Leftrightarrow \left\{ \begin{array}{lll} x & \equiv & 60^{181} \pmod{3^3} \\ x & \equiv & 60^{181} \pmod{11} \end{array} \right. \Leftrightarrow \left\{ \begin{array}{lll} x & \equiv & 3^{181} \cdot 20^{181} \pmod{3^3} \\ x & \equiv & 60^{181} \pmod{11} \end{array} \right. .$$

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

$$x \equiv 60^{181} \pmod{297} \Leftrightarrow \left\{ \begin{array}{lll} x & \equiv & 0 \pmod{3^3} \\ x & \equiv & 5 \pmod{11} \end{array} \right. ,$$

que tiene solución 27.

Segunda parte: Desarrollo

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

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

Ver notas de teórico.

b. Si $\operatorname{mcd}(a, b) = 1$ 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

$$\begin{cases} x \equiv 8 \pmod{56} \\ x \equiv 1 \pmod{21} \\ x \equiv 4 \pmod{36} \\ x \equiv 8 \pmod{49} \end{cases},$$

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

$$x \equiv 8 \pmod{56} \Leftrightarrow \begin{cases} x \equiv 8 \pmod{8} \\ x \equiv 8 \pmod{7} \end{cases} \Leftrightarrow \begin{cases} x \equiv 0 \pmod{8} \\ x \equiv 1 \pmod{7} \end{cases}, \tag{1}$$

$$x \equiv 1 \pmod{21} \Leftrightarrow \begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 1 \pmod{7} \end{cases} \Leftrightarrow \begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 1 \pmod{7} \end{cases}, \tag{2}$$

$$x \equiv 4 \pmod{36} \Leftrightarrow \begin{cases} x \equiv 4 \pmod{4} \\ x \equiv 4 \pmod{9} \end{cases} \Leftrightarrow \begin{cases} x \equiv 0 \pmod{4} \\ x \equiv 4 \pmod{9} \end{cases}. \tag{3}$$

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

$$\begin{cases} x \equiv 0 \pmod{8} \\ x \equiv 4 \pmod{9} \\ x \equiv 8 \pmod{49} \end{cases}$$

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

$$\begin{cases} x \equiv 1 \pmod{p} \\ \text{o} \\ x \equiv -1 \pmod{p} \end{cases} \text{ y } \begin{cases} x \equiv 1 \pmod{q} \\ \text{o} \\ x \equiv -1 \pmod{q} \end{cases} \text{ y } \begin{cases} x \equiv 1 \pmod{r} \\ \text{o} \\ x \equiv -1 \pmod{r} \end{cases}$$

por lo que

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

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

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

que son las 8 opciones posibles.

Primer parcial - 14 de mayo de 2014. Duración: 3 horas y media

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:

(1200)	1	0
(7)	0	1
$1200 = 7 \cdot 171 + 3$	1	-171
$7 = 3 \cdot 2 + 1$	-2	343

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 $mcd(50, 23) = 1$. 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 $mcd(6, 15) = 3$ 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 conguente 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 $mcd(5, 12) = 1 = mcd(2, 9)$.

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

En la segunda tenemos: $2x \equiv 5 \equiv 5+9 = 14 \pmod 9$, luego $x \equiv 7 \pmod 9$, ya que $mcd(2, 9) = 1$. 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

$$4k \equiv 4 \pmod 9 \quad \Rightarrow k \equiv 1 \pmod 9$$

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

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

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

Matemática Discreta 2
Curso 2013

Primer parcial

Ejercicio 1)

Sea S_a el sistema de congruencias

$$S_a \left\{ \begin{array}{lcl} x & \equiv & 2 (\bmod\ 3) \\ x & \equiv & 4 (\bmod\ 7) \\ x & \equiv & 5 (\bmod\ 11) \\ x & \equiv & a (\bmod\ 21) \end{array} \right.$$

a) Hallar el mínimo $a \in \mathbb{N}$ para 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.

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.

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

c) ¿Es cierto el recíproco? Caso afirmativo: demostrarlo. Caso ne-gativo: dar contraejemplo.

d) Se tiene un tablero de 18×20 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?

Ejercicio 3)

Sea ϕ la función de Euler.

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

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 $d = mcd(m, n)$.

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

c) Calcular $10 \cdot 17^{2306} (\text{mod } 60 \cdot 42)$.

4 de mayo de 2012.

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 $\mathbb{Z}$.

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

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

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

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.

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

SEGUNDO PARCIAL - 30 DE NOVIEMBRE DE 2017. DURACIÓN: 4 HORAS

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. Probar que 2 es raíz primitiva módulo 19.

b. Sea p es primo y g una raíz primitiva módulo p. Si m es el orden de g en $U(p^2)$, probar que $p-1 \mid m$.

c. Hallar una raíz primitiva módulo $19^2 = 361$.

d. Probar que si x es un entero impar y p es un primo impar, entonces que $x^m \equiv 1 \pmod{2p^2} \Leftrightarrow x^m \equiv 1 \pmod{p^2}$.

e. Hallar una raíz primitiva módulo 722.

Ejercicio 2. Sea $G = U(241)$ y $H = \{h \in G, \text{ tal que } o(h) \mid 24\}$.

a. Probar que si $x \notin H$ y $x^2 \in H$ entonces $o(x) \in \{16, 48\}$.

b. Probar que $\#H = 24$ (*sugerencia:* 241 *es primo*).

c. Probar que $H = \langle \overline{2} \rangle$ y listar los elementos de H.

d. Probar, utilizando lo anterior, que $o(\overline{11}) = 48$.

e. Sabiendo que $10^5 \equiv 2^{20} \pmod{241}$, hallar $o(\overline{10})$.

f. Hallar (justificando) una raíz primitiva módulo 241 (puede quedar expresada como producto de potencias).

g. Para utilizar el método Diffie Hellman de intercambio de 5 clave, Ana y Bruno eligen g una raìz primitiva módulo 241. Si Ana elige el exponente $a = 50$ y Bob elige el exponente $b = 56$, probar que la clave fijada es $k = 15$ o $k = 225$.

Ejercicio 3. Sea G un grupo y $H < G$. Consideramos en G la relación de equivalencia $g \sim k \Leftrightarrow gk^{-1} \in H$ (NO es necesario verificar que es relación de equivalencia).

a. Probar que si C es una clase de equivalencia, entonces $\#C = |H|$.

b. Probar que si $F : G \to A$ es un homomorfismo de grupos y $H = \ker(F)$ entonces para $g, k \in G$ se tiene que $g \sim k \Leftrightarrow F(g) = F(k)$.

c. Enunciar y demostrar el Teorema de órdenes para homomorfismos de grupos.

d. Probar que si $F : G \to A$ es un homomorfismo sobreyectivo entre grupos finitos, entonces $a^{|G|} = e_A$ para todo $a \in A$.

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

SEGUNDO PARCIAL - 29 DE JUNIO DE 2017. DURACIÓN: 3 HORAS

El parcial es *sin* material y *sin* calculadora.

Ejercicio 1. Sea $g \in G$ tal que $o(g) = n$

a. Probar que para todo $m \in \mathbb{Z}$ se cumple $g^m = e \Longleftrightarrow n \mid m$.

b. Probar que $g^a = g^b \Longleftrightarrow a \equiv b \pmod{n}$.

c. Probar que $|\langle g \rangle| = n$.

d. Usar el Teorema de Lagrange para probar que si G es finito, entonces $n \mid |G|$.

Solución.

a. $(\Rightarrow)$ Si $g^m = e$, dividiendo m entre n tenemos que $m = nq + r$ con $0 \leq r < n$. Por lo tanto $e = g^m = g^{nq+r} = (g^n)^q\, g^r = e^q\, g^r = g^r$. En otras palabras $g^r = e$, pero n es el menor entero positivo que cumple $g^n = e$, y como $0 \leq r < n$ debe ser $r = 0$. Luego, $m = nq$ y $n \mid m$.

$(\Leftarrow)$ Si $m = nq$, entonces $g^m = g^n q = (g^n)^q = e^q = e$.

b. $g^a = g^b \Leftrightarrow g^{a-b} = e \overset{\textbf{(a)}}{\Longleftrightarrow} n \mid a - b \Leftrightarrow a \equiv b \pmod{n}$.

c. Por la parte anterior $\langle g \rangle = \{g^k \ : \ k \in \mathbb{Z}\} = \{g^0, g^1, \ldots, g^{n-1}\}$, donde los elementos $g^0, g^1, \ldots, g^{n-1}$ son todos distintos. Concluimos que $|\langle g \rangle| = n$.

d. Como $\langle g \rangle$ es un subgrupo de G, el Teorema de Lagrange implica que $n = |\langle g \rangle| \mid |G|$.

Ejercicio 2.

a. Probar que 11 es una raiz primitiva módulo 71.

b. Aldo y Beatriz eligen $p = 71$ y $g = 11$ para intercambiar claves utilizando el método de Diffie y Hellman. Beatriz elige $m = 7$ y Aldo le envía el número $g^n \equiv 61 \pmod{71}$. ¿Cuál es la clave que acuerdan?

Solución.

a. Como 71 es primo $\varphi(71) = 70 = 2 \cdot 5 \cdot 7$. Entonces alcanza probar que $11^{10} \not\equiv 1 \pmod{71}$, que $11^{14} \not\equiv 1 \pmod{71}$, y que $11^{35} \not\equiv 1 \pmod{71}$. En efecto calculamos $11^2 \equiv 50$, $11^4 \equiv 50^2 \equiv 15$, $11^8 \equiv 15^2 \equiv 12$, $11^{16} \equiv 12^2 \equiv 2$, $11^{32} \equiv 2^2 \equiv 4$. Ahora $11^{10} \equiv 11^8 \cdot 11^2 \equiv 32 \not\equiv 1$, $11^{14} \equiv 11^{10} \cdot 11^4 \equiv 54 \not\equiv 1$, y $11^{35} \equiv 11^{32} \cdot 11^2 \cdot 11 \equiv 70 \not\equiv 1$.

b. La clave que acuerdan es $g^{nm} = (g^n)^m \equiv 61^7 \pmod{71}$. Calculamos $61^2 \equiv 29$, $61^4 \equiv 29^2 \equiv 60$, y tenemos $61^7 \equiv 61 \cdot 61^2 \cdot 61^4 \equiv 60 \cdot 10 \cdot 29 \equiv 66 \pmod{71}$.

Ejercicio 3. Alicia y Beto quieren comunicarse con el método ElGamal. A tales efectos eligen un primo p y una raíz primitiva g módulo p. Alicia elige un entero a como su clave privada y calcula $h \equiv g^a \pmod{p}$ como su clave pública. Beto quiere enviar un mensaje $m \in \mathbb{Z}_p$ a Alicia.

a. Describir el algoritmo de cifrado E que debe usar Beto.

b. Describir la función de descifrado D que debe usar Alicia.

c. Demostrar que $D(E(m)) = m$ para todo $m \in \mathbb{Z}_p$.

Solución.

a. Beto elige un entero b secreto (utilizable una única vez) y calcula $r \equiv g^b \pmod{p}$ y $c \equiv h^b \cdot m \pmod{p}$, obteniendo $E(m) = (r, c)$.

b. Ana calcula $D(r, c) = c \cdot r^{-a} \pmod{p}$

c. $D(E(m)) \equiv D(g^b, h^b \cdot m) \equiv (h^b \cdot m) \cdot (g^b)^{-a} \equiv (g^a)^b \cdot m \cdot g^{-ab} \equiv m \cdot (g^{ab} \cdot g^{-ab}) \equiv m \pmod{p}$

Ejercicio 4. Consideramos el grupo dihedral D_3.

a. Describir todos los elementos de D_3 indicando su orden.

b. Sean $u, v \in D_3$ dos elementos distintos de orden 2. Probar que uv tiene orden 3.

c. Consideramos la función $f : D_3 \to D_3$ dada por $f(x) = x^2$. ¿Es f un homomorfismo?

d. Describir todos los homomorfismos $h : \mathbb{Z}_6 \to D_3$.

Solución.

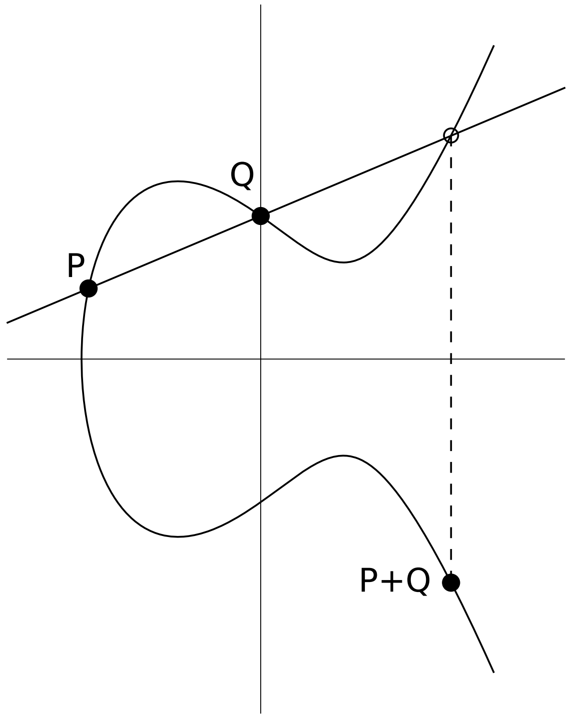
a. $D_3 = \{e, r, r^2, s, sr, sr^2\}$ donde r y r^2 son rotaciones y tienen orden 3, mientras que s, sr y sr^2 son simetrías axiales y tienen orden 2.

b. Como u y v tienen orden 2 son simetrías axiales. Entonces uv es un movimiento directo, debiendo ser 1, r, o r^2. Pero $u \neq v$ implica que $uv \neq e$. Entonces uv es una rotación, luego tiene orden 3.

c. No es un homomorfismo, por ejemplo si u y v son como en la parte anterior $f(u) = e$ y $f(v) = e$, pero $f(uv) = (uv)^2 \neq e$.

d. Como $\mathbb{Z}_6$ es cíclico generado por $\overline{1}$ de orden 6, cualquier homomorfismo es de la forma $h(\overline{n}) = g^n$ para algún $g \in D_3$ con $o(g) \mid 6$. Pero esto último vale para cualquier $g \in D_3$, entonces hay 6 homomorfismos $h : \mathbb{Z}_6 \to D_3$, uno para cada posible g.

Bonus. Determinar geométricamente el punto $\mathsf{P} + \mathsf{Q}$ en la siguiente curva elíptica:



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

Solución cuarta prueba (segundo parcial) - 1 de diciembre de 2016.

Ejercicio 1. (15 puntos) *(Ejercicio 1 del segundo parcial del curso semipresencial de 2015)*

a. Probar que 2 es raíz primitiva módulo 53.

b. Hallar todos los $x \in \mathbb{Z}$ tales que $x^{19} \equiv 32 (\text{mód } 53)$.

c. Archibaldo y Baldomero quieren pactar una clave común empleando el protocolo Diffie-Hellman. Para ésto fijan el primo $p = 53$ y la raíz primitiva $g = 2$. Archibaldo selecciona el número $m = 28$ y le remite el número 49 a Baldomero. Éste selecciona el número $n = 5$. ¿Cuál es la clave común k que acordaron Archibaldo y Baldomero?

Solución Ejercicio 1:

a. Observemos primero que $52 = 2^2 \cdot 13$. Por lo tanto, si queremos probar que 2 es raíz primitva módulo 53, debemos probar que $2^{\frac{52}{p}} \not\equiv 1 (\text{mód } 53)$, para todo p primo, con $p|52$. O sea debemos calcular 2^4 y 2^{26}.

n	$2^n \pmod{53}$
0	$1 \pmod{53}$
1	$2 \pmod{53}$
2	$4 \pmod{53}$
3	$8 \pmod{53}$
4	**16 mód53**
5	$32 \pmod{53}$
6	$11 \pmod{53}$
7	$22 \pmod{53}$
8	$44 \pmod{53}$
9	$35 \pmod{53}$
10	$17 \pmod{53}$
11	$34 \pmod{53}$
12	$15 \pmod{53}$
13	$30 \pmod{53}$
14	$7 \pmod{53}$
15	$14 \pmod{53}$
$\vdots$	$\vdots$

Luego $2^{26} = 2^{13} \times 2^{13} \equiv 900 \pmod{53} \equiv -1 \pmod{53}$.
Entonces 2 es raíz primitiva módulo 53.

b. Como $32 = 2^5$ la ecuación a resolver se transforma en: $x^{19} \equiv 2^5 (\text{mód } 53)$. Por otro lado, como 2 es raíz primitva módulo 53, entonces para todo $x \in \mathbb{Z}$ existe $0 \leq t(x) \leq 52$ tal que $x = 2^{t(x)}$. Luego la ecuación a resolver se transforma en: $2^{t(x)^{19}} \equiv 2^5 (\text{mód } 53)$. Nuevamente como 2 es raíz primitiva, la ecuación anterior es equivalente a: $19 \cdot t(x) \equiv 5 \pmod{52}$. Esto último a su vez es equivalente a $t(x) \equiv 3 \pmod{52}$. Luego $x = 2^3 \pmod{53}$, o sea $x = 8 + 53 \cdot z$, con $z \in \mathbb{Z}$.

c. Archibaldo toma $m = 28$ y le envía $2^{28} \equiv 49 \pmod{53}$ a Baldomero. Éste toma $m = 5$ y le envía $49^5 \pmod{53}$ a Archibaldo. O sea, $49^5 \equiv (-4)^5 \pmod{53} = -2^{10} \pmod{53} \equiv -17 \pmod{53} \equiv 36 \pmod{53}$. O sea que la clave común acrodada es $k = 36$.

Ejercicio 2. (20 puntos)

a. Calcular el número de raíces primitivas en $U(29)$.

b. Encontrar todas las raíces primitivas de $U(29)$.
(Sugerencia: Calcular $2^n \pmod{29}$, para todo $0 \leq n \leq 14$, para faciitar los cálculos posteriores.)

c. Ordenar en forma creciente las raíces primitivas halladas en el ítem anterior: $r_1 \leq r_2 \leq r_3 \leq r_4 \leq r_5 \leq .....$ Luego escribir la secuencia: $r_1 r_5 0 r_9 r_3 r_1 r_7$. Finalmente traducir usando la numeración de los símbolos:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	␣
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27

d. Utilizando el método de Vigenère **decodificar** el siguiente texto, usando la palabra clave hallada en el ítem anterior:

OZ␣LPTSOKMS␣BUCBRSNCG

Solución Ejercicio 2:

a. El número de raíces primitvas en $U(n)$ (si hay) es $\varphi(\varphi(n))$, siendo φ la función de Euler. En este caso $\varphi(29) = 28$, pues 29 es primo. Luego $\varphi(28) = \varphi(4 \times 7) = \varphi(4) \cdot \varphi(7) = 2 \cdot 6 = 12$. Entonces el número de raíces primitvas en $U(29)$ es 12.

b. Para encontrar todas las raíces primitivas calculamos los valores sugeridos en la letra del ejercicio, en la siguiente tabla:

n	$2^n \pmod{29}$
0	$1 \pmod{29}$
1	$2 \pmod{29}$
2	$4 \pmod{29}$
3	$\mathbf{8 \bmod 29}$
4	$16 \pmod{29}$
5	$\mathbf{3 \bmod 29}$
6	$6 \pmod{29}$
7	$12 \pmod{29}$
8	$24 \pmod{29}$
9	$\mathbf{19 \bmod 29}$
10	$9 \pmod{29}$
11	$\mathbf{18 \bmod 29}$
12	$7 \pmod{29}$
13	$\mathbf{14 \bmod 29}$
14	$-1 \pmod{29}$
$\vdots$	$\vdots$

Luego se concluyen varias cosas de la tabla anterior:

- Por un lado $2^{14} \not\equiv 1 \pmod{29}$ y también se verifica: $2^4 \not\equiv 1 \pmod{29}$. Entonces $o(2) = 28$, concluyendo que 2 es raíz primitiva en $U(29)$.
- Como 2 es raíz primitiva, entonces $2^s \pmod{29}$ es raíz primitiva para todo $s \in \mathbb{N}$ tal que $\text{mcd}(s, 28) = 1$. Entonces las que están marcadas en "negrita" en la tabla son también raíces primitivas. Así que tenemos hasta ahora las siguientes raíces primitivas: 2, 3, 8, 14, 18 y 19.

- Por último puede observarse que $-2, -3, -8, -14, -18$ y -19 son raíces primitivas de $U(29)$. O sea, $27, 26, 21, 15, 11$ y 10 son raíces primitivas de $U(29)$. Sugerimos tres caminos para probar la última afirmación.
  - Completar la tabla anterior hasta $n = 28$.
  - Probar teóricamente que si a es raíz primitva en $U(29)$ entonces $(-a)$ también.
  - Hacer las cuentas a mano en cada caso.

c. Por lo tanto las raíces primitivas, ordenadas en forma creciente son:

$$2 \leq 3 \leq 8 \leq 10 \leq 11 \leq 14 \leq 15 \leq 18 \leq 19 \leq 21 \leq 26 \leq 27.$$

La palabra clave es: CLASICO (sería CLÁSICO).

d. Por último decodificando el mensaje oculto

$$OZ\_LPTSOKMS\_BUCBRSNCG$$

utilizando Vigenère, obtenemos el mensaje:

$$NO\_TIREN\_MAS\_GARRAFAS$$

Ejercicio 3. (10 puntos) Describir el "Método de Fermat" de ataque al RSA, y demostrar la validez del algoritmo planteado.

Solución Ejercicio 3

Ver los apuntes de Teórico, Capítulo 5, ítem 5.3.4, Método de Fermat de ataque al RSA.

Segundo parcial - 29 de junio de 2016.

Primera parte: Múltiple Opción

Ejercicio 1. Austria y Bielorusia quieren acordar una clave común utilizando el protocolo Diffie-Hellman. Para ello toman el primo $p = 499$ y $g = 7$ raíz primitiva módulo p. Austria elije el número $m = 394$ y le envía el número 489 a Bielorusia. Bielorusia elije el número $n = 18$. ¿Cuál es la clave k común que acordaron Austria y Bielorusia?
Indicar cuál de las opciones es correcta:

A. $k = 331$. **B.** $k = 77$. **C.** $k = 80$. **D.** $k = 64$.

Solución:
Tenemos que calcular $489^{18} \pmod{499} \equiv (-10)^{18} \pmod{499} \equiv ((-10)^3)^6 \pmod{499} \equiv (-1000)^6 \pmod{499} \equiv (-2)^6 \pmod{499} \equiv 64 \pmod{499}$.

Ejercicio 2. Sean $n = 209$ y $e = 7$. Para los datos anteriores sea función de descifrado $D : \mathbb{Z}_n \to \mathbb{Z}_n$ definida por el protocolo RSA. Indicar cuál de las opciones es correcta:

A. $D(y) = y^{103} \pmod{n}$.

B. $D(y) = y^{30} \pmod{n}$.

C. $D(y) = y^{119} \pmod{n}$.

D. $D(y) = y^{163} \pmod{n}$.

Solución:
La función de descifrado es $D(y) = y^d \pmod{n}$ donde d es tal que $d \equiv e^{-1} \pmod{\varphi(n)}$. La factorización de n es $209 = 11 \cdot 19$, por lo que $\varphi(11 \cdot 19) = 10 \cdot 18 = 180$. Utilizando el algoritmo extendido de Euclides obtenemos $d \equiv 103 \pmod{180}$.

Segunda parte: Desarrollo

Ejercicio 3.

a. Sea $(G, *)$ un grupo finito y H un subgrupo de G. Definimos la siguiente relación en G:

$$g \sim g' \Leftrightarrow g * (g')^{-1} \in H.$$

Probar que la relación definida es una relación de equivalencia.

b. Sean G, K grupos finitos y $f : G \to K$ un homomorfismo de grupos. Probar que $\operatorname{Ker}(f)$ es un subgrupo de G.

c. Probar el teorema de órdenes para grupos:

Sean G y K dos grupos finitos y $f : G \to K$ un homomorfismo de grupos. Entonces

$$|G| = |\operatorname{Ker}(f)||\operatorname{Im}(f)|.$$

Solución: Ver la segunda demostración del Teorema de Ordenes de las notas, Teorema 3.9.8.

Ejercicio 4.

a. Sean G un grupo finito, $g \in G$ y $n \in \mathbb{N}$, probar que $\mathrm{o}\left(g^{n}\right)=\frac{\mathrm{o}(g)}{\operatorname{mcd}(\mathrm{o}(g), n)}$.
Solución: Ver Proposición 3.7.8 parte 7 de las notas.

b. Probar que 2 es raíz primitiva módulo 101 y hallar un elemento de $U(101)$ con orden 10.
Solución: Para ver que 2 es r.p. módulo 101, alcanza con ver $2^{50} \not\equiv 1 \pmod{101}$ y $2^{20} \not\equiv 1 \pmod{101}$, ya que $\varphi(101)=100=2^{2} 5$ y $100/2=50$, $100/5=20$. Entonces $2^{20}=(2^{10})^{2} \equiv (1024)^{2} \pmod{101} \equiv 14^{2} \pmod{101} \equiv 196 \pmod{101} \equiv 95 \pmod{101} \not\equiv 1 \pmod{101}$. También $2^{50}=(2^{20})^{2} \cdot 2^{10} \equiv (95)^{2} \cdot 14 \pmod{101} \equiv (-6)^{2} \cdot 14 \pmod{101} \equiv 36 \cdot 14 \pmod{101} \equiv 504 \pmod{101} \equiv -1 \pmod{101}$. Con es probamos que 2 es r.p. módulo 101.
Para hallar un elemento de orden 10 utilizamos la parte anterior y el hecho que que el orden de 2 es 100. Utilizamos $n=10$ y obtenemos

$$\mathrm{o}\left(2^{10}\right)=\frac{\mathrm{o}(2)}{\operatorname{mcd}(\mathrm{o}(2), 10)}=\frac{100}{\operatorname{mcd}(100,10)}=\frac{100}{10}=10.$$

Por lo tanto $\mathrm{o}(14)=10$.

Ejercicio 5. Sean los grupos $G=\mathbb{Z}_{100}$ y $K=U(101)$.

a. Probar que los grupos G y K son isomorfos.
Solución: Dado que $\overline{1}$ es generador de G y tiene orden 100 que es el orden de 2 en K, el morfismo $f: G \rightarrow K$ dado por $f(\bar{n})=2^{n} \pmod{101}$ es un morfismo bien definido. Es fácil ver que es inyectivo ya que $f(n)=1$ si y solo si $2^{n} \equiv 1 \pmod{101}$, o sea si $n \equiv 0 \pmod{100}$. Como G y K tienen igual orden entonces es biyectivo y por lo tanto es un isomorfismo.

b. Describir todos los isomorfismos entre G y K.
Solución: En la parte anterior podemos cambiar f por f_{k} donde $f_{k}(n)=2^{kn} \pmod{101}$ y k otro elemento de orden 100 de $\mathbb{Z}_{100}$. El nuevo f_{k} es isomorfismo de igual manera que antes. Por el ejercicio anterior vemos que los k que cumplen que son generadores de $\mathbb{Z}_{100}$ son los que cumplen $\operatorname{mcd}(k, 100)=1$. Y por lo tanto obtuvimos todos los isomorfismos entre G y K.

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

Primer parcial - 3 de diciembre de 2015. Duración: 3 horas

N° de parcial	Cédula	Apellido y nombre

Ejercicio 1.

a. Probar que 2 es raíz primitiva módulo 53.

b. Hallar todos los $x \in \mathbb{Z}$ tales que $x^{19} \equiv 32 \pmod{53}$.

c. Archibaldo y Baldomero quieren pactar una clave común empleando el protocolo Diffie-Hellman. Para ésto fijan el primo 53 y la raíz primitiva $g = 2$. Archibaldo selecciona el número $m = 28$ y le remite el número 49 a Baldomero. Baldomero selecciona el número $n = 5$. ¿Cuál es la clave k común que acordaron Archibaldo y Baldomero?

Ejercicio 2.

a. Sea $(G, *)$ un grupo finito y H un subgrupo de G. Definimos la siguiente relación en G:

$$g \sim g' \Leftrightarrow g * (g')^{-1} \in H.$$

Probar que la relación definida es una relación de equivalencia.

b. Sean G, K grupos finitos y $f : G \to K$ un homomorfismo de grupos. Probar que $\operatorname{Ker}(f)$ es un subgrupo de G.

c. Probar el teorema de órdenes para grupos:

Sean G y K dos grupos finitos y $f : G \to K$ un homomorfismo de grupos. Entonces

$$|G| = |\operatorname{Ker}(f)||\operatorname{Im}(f)|.$$

Ejercicio 3.

a. Sea $f : G \to K$ un homomorfismo de grupos y $g \in G$ un elemento de orden $o(g)$ finito. Probar que $o(f(g)) \mid o(g)$.

b. Para los pares de grupos G y K, determinar si existen homomorfismos no triviales $f : G \to K$. Si existen encontrarlos todos, de lo contrario justificar por qué no existen.

- **i)** $G = \mathbb{Z}_6$ el grupo de enteros módulo 6 y $K = S_3$ el grupo de permutaciones de 3 elementos.
- **ii)** $G = S_6$ el grupo de permutaciones de 6 elementos y $K = \mathbb{Z}_7$ el grupo de enteros módulo 7.

c. Sean $G = D_{12}$ el grupo dihedral y $K = S_3 \times U(8)$ el producto cartesiano de los grupos S_3 (permutaciones de 3 elementos) y $U(8)$ ¿Son isomorfos estos grupos? De serlo, dar un isomorfismo entre ellos, de lo contrario justificar por qué no lo son.

Segundo parcial - 4 de julio de 2014. Duración: 3 horas y media

N° de parcial	Cédula	Apellido y nombre	Salón

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	␣
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27

Ejercicio 1.

a. Sea $n \in \mathbb{Z}^+$, y g un entero coprimo con n. Probar que si a es el orden de $\overline{g}$ en $U\left(n^2\right)$ y b es el orden de $\overline{g}$ en $U(n)$, entonces $b \mid a$.

b. Sea $p = 19$.

i) Probar que 10 es raíz primitiva módulo p.

ii) ¿Es 10 raíz primitiva módulo p^2? Pueden utilizar los siguientes datos: $10^5 \equiv 3 \pmod{p^2}$ y $3p^2 = 1083$.

iii) Para cada $k \in \mathbb{Z}^+$ hallar una raíz primitiva módulo $2p^k$.

Ejercicio 2.

a. Si $f : G \to K$ es un homomorfismo de grupos probar que $o(f(g)) \mid o(g)$ para todo $g \in G$.

b. En cada parte, hallar todos los homomorfismos $f : G \to K$ justificando debidamente.

i) $G = S_4$ con la composición como operación y $K = \mathbb{Z}_{35}$ con la suma de clases como operación.

ii) $G = \mathbb{Z}_{15}$ y $K = \mathbb{Z}_6$, ambos grupos con la suma de clases como operación.

Ejercicio 3. Sea G un grupo y $g \in G$ de orden finito. Probar que:

a. Si $k \in \mathbb{Z}^+$, entonces $o(g^k) = \dfrac{o(g)}{\operatorname{mcd}(o(g), k)}$.

b. Si $H = \langle g \rangle$, entonces existen $\varphi(o(g))$ elementos en H que generan H.

Ejercicio 4.

a. Ana y Bruno quieren acordar una clave común usando el protocolo Diffie-Hellman. Para ello eligen el primo $p = 1009$ y la raíz primitiva $g = 11$. Ana elige el número $m = 260$ le envía a Bruno el número 1005. Bruno elige el entero $n = 8$. ¿Cuál es la clave k común que acordaron Ana y Bruno?.

b. Ahora Ana quiere comunicarse con Bruno través de un sistema Vigenere donde la palabra clave consiste de 3 letras de la siguiente manera: se toma la clave k común acordada en la parte anterior y se la escribe en base 28:

$$k = L_2 28^2 + L_1 28 + L_0.$$

Luego la clave común resulta de sustituir en $L_2L_1L_0$ por sus respectivas letras (por ejemplo si $k = 25 \cdot 28^2 + 0 \cdot 28 + 2$ entonces la clave común será `YAC`).

i) Calcular la clave k como $L_2L_1L_0$.

ii) Usando la clave anterior descifrar el siguiente mensaje: `WUFAGHFCWÑKZBXHEÑ␣DXMUG`.

Ejercicio 5. Enunciar y demostrar el Teorema de Lagrange para grupos.

Universidad de la República - Facultad de Ingeniería - IMERL.
Matemática Discreta 2

Examen - 8 de febrero de 2018.

Ejercicio 1.

a. Sean $0 \neq a$, $b \in \mathbb{Z}$, probar que

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

Solución: Ver Proposición 1.2.6 de las notas teóricas.

b. Sean $a, b \in \mathbb{Z}$, probar que la ecuación diofántica $ax + by = c$ tiene solución si y solo si $\operatorname{mcd}(a, b)|c$.

Solución: Ver la parte 1 del teorema 1.5.3 de las notas teóricas

c. Hallar todas las soluciones módulo 62 de la ecuación

$$26x \equiv 262 \pmod{62}.$$

Solución: Como $262 \equiv 14 \pmod{62}$, debemos resolver $26x \equiv 14 \pmod{62}$. Por definición de congruencia, es equivalentema resolver la diofántica

$$26x + 62y = 14$$

y dividiendo todo entre 2, obtenemos la diofántica equivalente

$$13x + 31y = 7.$$

Aplicando el algoritmo extendido de Euclides obtenemos que $13(12) + 31(-5) = 1$ y por lo tanto (multiplicando por 7) obtenemos que $13(12\cdot 7) + 31(-5\cdot 7) = 7$. Entonces la diofántica $13x + 31y = 7$ tiene solución particular $(x_0,\, y_0) = (84, -35)$ y todas sus soluciones son de la forma $(x,\, y) = (84 + 31k,\, -35 - 13k)$ para k entero. Por lo tanto

$$x = 84 + 31k \equiv 22 + 31k \pmod{62},\ k \in \mathbb{Z},$$

y tomando $k = 0, 1$ obtenemos todas las posibles soluciones módulo 62, que son 22 y $22 + 31 = 53$.

Ejercicio 2.

a. Resolver los siguientes sistemas de congruencias:

i) $\begin{cases} x \equiv 0 \pmod{11} \\ x \equiv 8 \pmod{17} \end{cases}$ ii) $\begin{cases} x \equiv 33 \pmod{44} \\ x \equiv 25 \pmod{34} \end{cases}$

Solución:

i) Si escribimos $x = 17t+8$, $t \in \mathbb{Z}$, y lo sustituímos en la primer congruencia, obtenemos $17t + 8 \equiv 0 \pmod{11}$. Por lo tanto $6t \equiv 3 \pmod{11}$ y como 3 es coprimo con 11 podemos cancelarlo y obtenemos $2t \equiv 1 \pmod{11}$, por lo tanto $t = 6$ y $x \equiv 17 \cdot 6 + 8 \pmod{11 \cdot 17} \equiv 110 \pmod{11 \cdot 17}$.

ii) Si escribimos $44 = 4 \cdot 11$ y $34 = 2 \cdot 17$ podemos aplicar el TCR a ambas congruencias para obtener el siguiente sistema equivalente al planteado

$$\begin{cases} x \equiv 33 \pmod{4} \equiv 1 \pmod{4} \\ x \equiv 33 \pmod{11} \equiv 0 \pmod{11} \\ x \equiv 25 \pmod{2} \equiv 1 \pmod{2} \\ x \equiv 25 \pmod{17} \equiv 8 \pmod{17} \end{cases}$$

Como la primer congruencia de este sistema implica la tercera, podemos eliminar la tercera. Además, usando la parte anterior, el sistema nos queda equivalente

$$\begin{cases} x \equiv 1 \pmod{4} \\ x \equiv 110 \pmod{11 \cdot 17} \end{cases}$$

que tiene solución 297.

b. Sean p y q dos primos distintos. Describir el criptosistema RSA usando p y q (especificar cuáles datos son públicos y cuáles privados y definir las funciones E y D de cifrado y descifrado respectivamente).
Solución: Ver notas teóricas.

c. Probar que en el criptosistema RSA, la función de descifrado D es la función inversa de la función de cifrado E.
Solución: Ver Proposición 5.3.1 de las notas teóricas.

d. Mostrar con un ejemplo por qué, en el sistema RSA, es necesario que los primos p y q sean distintos.
Solución: Si tomamos $x = p$ y $e > 1$, cuando aplicamos la función E obtenemos $E(p) = p^e \pmod{p^2} = 0$; entonces al aplicar la función de descifrado al 0 deberíamos obtener p. Pero $D(0) = 0^d = 0 \neq p \pmod{p^2}$ y entonces $D(E(p)) \neq p$.

e. Con los primos 11 y 17 utilizar el criptosistema RSA con $e = 171$ para cifrar el número $x = 121$.
Solución: Tenemos que calcular $x = 121^{171} \pmod{11 \cdot 17}$. Como $\operatorname{mcd}(121, 11 \cdot 17) = 11 \neq 1$, no podemos aplicar Euler en esta congruencia. Como $\operatorname{mcd}(11, 17) = 1$, por el TCR, la congruencia es equivalente al sistema

$$\begin{cases} x \equiv 121^{171} \pmod{11} \equiv 11^{2\cdot 171} \pmod{11} \equiv 0 \pmod{11} \\ x \equiv 121^{171} \pmod{17} \equiv 11^{2\cdot 171} \pmod{17} \end{cases}$$

Para la segunda congruencia podemos aplicar Euler y como $\varphi(17) = 16$ y $2 \cdot 171 \equiv 6 \pmod{16}$, tenemos que $x \equiv 11^6 \pmod{17} \equiv (-6)^6 \equiv (36)^3 \equiv 2^3 \pmod{17} \equiv 8 \pmod{17}$. Por lo tanto tenemos que resolver el sistema

$$\begin{cases} x \equiv 0 \pmod{11} \\ x \equiv 8 \pmod{17} \end{cases},$$

que por la primer parte del ejercicio sabemos que es 110, por lo tanto $E(121) = 110$.

Otro camino para reducir la 2da. ecuación poría haber sidp, a partir de $x \equiv (121)^{171} \pmod{17} \equiv 2^{171} \pmod{17}$, aplicando Euler obtenemos $x \equiv 2^{11} \equiv 2^{2^4+2^1+2^0} \pmod{17}$. Utilizamos el método de exponenciación rápida para obtener las potencias $2^{2^k} \pmod{17}$, $k = 0, 1, 2, 3, 4$. Primero $2^{2^0} = 2$, luego $2^{2^1} = 2^2 = 4$, $2^{2^2} = 16 \equiv -1 \pmod{17}$, $2^{2^3} \equiv 2^{2^4} \pmod{17} \equiv 1 \pmod{17}$. Por lo tanto $2^{11} \equiv 2 \cdot 4 \cdot 1 \pmod{17} \equiv 8 \pmod{17}$.

Ejercicio 3.

a. Definir grupo.
Solución: Ver notas teóricas.

b. Sea $(G, \times)$ un grupo, probar que el neutro es único.
Solución: Ver notas teóricas.

c. Sea $(G, \times)$ un grupo y $g \in G$, probar que el inverso de g es único.
Solución: Ver notas teóricas.

d. Sean G y K dos grupos y $f : G \to K$ un homomorfismo. Probar que si $g \in G$ es un elemento de orden finito entonces

$$\mathrm{o}(f(g)) \mid \mathrm{o}(g).$$

Solución: Ver notas teóricas.

e. Hallar todos los homomorfismos $f : U(13) \to \mathbb{Z}_9$ (sugerencia: hallar una raíz primitiva módulo 13).
Solución: Veamos primero que 2 es raiz primitiva módulo 13. Sabemos que $\varphi(13) = 12 = 2^2 3$. Hay que probar que $2^4, 2^6 \not\equiv 1 \pmod{13}$. Veamos eso, $2^4 = 16 \equiv 3 \pmod{13}$ y $2^6 \equiv 3 \cdot 4 \pmod{13} \equiv -1 \pmod{13}$.
Como $U(13)$ es cíclico, todos los homomorfismos son $f\left(2^k\right) = k \cdot n$, con $\mathrm{o}(n) | \mathrm{o}(2) = 12$, $n \in \mathbb{Z}_9$. Estos elementos son $0, 3, 6$ cuyos ordenes son $1, 3, 3$. Por lo tanto tenemos 3 homomorfismos.

Universidad de la República - Facultad de Ingeniería - IMERL.
Matemática Discreta 2

EXAMEN - 20 DE DICIEMBRE DE 2017.

Ejercicio 1.

a. Definir la función φ de Euler.
Ver notas teóricas.

b. Enunciar y demostrar el Teorema de Euler.
Ver notas teóricas.

c. **i**) Probar que 127 es primo.
Solución: Como $127 < 13^2$ alcanza con probar que 127 no es divisible por los primos $2, 3, 5, 7$ y 11. Veamos eso: $127 = 63 \cdot 2 + 1$, $127 = 42 \cdot 3 + 1$, $127 = 25 \cdot 5 + 2$, $127 = 18 \cdot 1$ y $127 = 11 \cdot 11 + 6$.

ii) Hallar $0 \leq x < 127$ tal que $x \equiv 3^{502} \pmod{127}$.
Solución: Como $\operatorname{mcd}(3, 127) = 1$ podemos aplicar el Teorema de Euler. Como 127 es primo sabemos que $\varphi(127) = 126$ y $502 = 126 \cdot 3 + 124 \equiv -2 \pmod{126}$. Por lo tanto $3^{502} \equiv 3^{-2} \pmod{127} \equiv 9^{-1} \pmod{127}$. Utilizando el Algoritmo extendido de Euclides vemos que $1 = 9 \cdot (-14) + 127 \cdot 1$ de donde deducimos que

$$3^{504} \equiv 9^{-1} \pmod{127} \equiv -14 \pmod{127} \equiv 113 \pmod{127}.$$

d. Hallar $0 \leq x < 363$ tal que $x \equiv 12^{332} \pmod{363}$.
Solución: En este caso no podemos aplicar el Teorema de Euler ya que $\operatorname{mcd}(12, 363) = 3$. Pero podemos aplicar el teorema chino del resto de la siguiente manera:

$$x \equiv 12^{332} \pmod{363} \Leftrightarrow \begin{cases} x \equiv & 12^{332} \pmod{3} \\ x \equiv & 12^{332} \pmod{11^2} \end{cases}$$

Claramente $12^{332} \equiv 0 \pmod{3}$, por lo que falta reducir la otra congruencia. Sabemos que $\varphi(11^2) = 11 \cdot 10 = 110$ y $\operatorname{mcd}(12, 11^2) = 1$, aplicando el Teorema de Euler vemos que $12^{332} \equiv 12 \equiv 12^2 \pmod{11^2} \equiv 144 \pmod{11^2} \equiv 23 \pmod{11^2}$. Tenemos que resolver entonces:

$$\begin{cases} x \equiv & 0 \pmod{3} \\ x \equiv & 23 \pmod{11^2} \end{cases},$$

que tiene solución $23 + 11^2$. Por lo tanto $x = 23 + 11^2 = 144$.

Ejercicio 2.

a. Sea G un grupo abeliano y $x, y \in G$ tales que $\mathrm{o}(x) = ab$, con a, $b \in \mathbb{Z}^+$.

i) Probar que $\mathrm{o}\left(x^a\right) = b$.
Solución: Alcanza con probar que $\left(x^a\right)^b = e$ y que si $\left(x^a\right)^c = e$ entonces $b|c$.
Veamos la primer afirmación: $\left(x^a\right)^b = x^{ab} = e$ ya que $\mathrm{o}(x) = ab$. Si $\left(x^a\right)^c = e$ entonces $x^{ac} = e$ y $ab|ac$ de donde concluimos que $b|c$.

ii) Probar que si x e y tienen órdenes coprimos entonces $\mathrm{o}(xy) = \mathrm{o}(x)\mathrm{o}(y)$. **Solución:** Ver notas teóricas: Lema 4.1.7

b. Sea G el grupo de invertibles módulo 157, $G = U(157)$.

i) Sabiendo que en G, $\mathrm{o}(16) = 13$ y que $2^{12} \equiv 14 \pmod{157}$, hallar el orden de 2 en G.
Solución: $\mathrm{o}(2^4) = 13 \Rightarrow \dfrac{\mathrm{o}(2)}{\mathrm{mcd}(\mathrm{o}(2), 4)} = 13 \Rightarrow \mathrm{o}(2) = 13\,\mathrm{mcd}(\mathrm{o}(2), 4)$. Y como $\mathrm{mcd}(\mathrm{o}(2), 4) \in \{1, 2, 4\}$ tenemos que $\mathrm{o}(2) \in \{13, 26, 52\}$. Por letra $2^{12} \equiv 14 \pmod{157} \Rightarrow 2^{13} \equiv 28 \pmod{157} \Rightarrow \mathrm{o}(2) \neq 13$. También $2^{26} = (2^{13})^2 \equiv (28)^2 \pmod{157} \equiv 156 \pmod{157} \Rightarrow \mathrm{o}(2) \neq 26$ y por lo tanto $\mathrm{o}(2) = 52$.

ii) Sabiendo que $2^{46} \equiv 27 \pmod{157}$ hallar el orden de 3 en G.
Solución $\mathrm{o}(3^3) = \mathrm{o}(27) = \mathrm{o}(2^{46}) = \dfrac{\mathrm{o}(2)}{\mathrm{mcd}(\mathrm{o}(2), 46)} = \dfrac{52}{\mathrm{mcd}(52, 46)} = 26$, y como $\mathrm{o}(3^3) = \dfrac{\mathrm{o}(3)}{\mathrm{mcd}(\mathrm{o}(3), 3)}$ tenemos que $\mathrm{o}(3) = 26\,\mathrm{mcd}(\mathrm{o}(3), 3)$
Si $\mathrm{mcd}(\mathrm{o}(3), 3) = 1$ tendríamos que $\mathrm{o}(3) = 26$; calculamos entonces 3^{26}:
$3^{26} = 3^{24}3^2 = (3^3)^8 9 \equiv (2^{46})^8 9 \equiv 2^{368}9 \equiv (2^{52})^7 2^4 9 \equiv (1)^7 16(9) \equiv 144 \pmod{157} \neq 1$ por lo que $\mathrm{o}(3) \neq 26$ y entonces $\mathrm{o}(3) = 78$.

iii) Hallar una raíz primitiva módulo 157.
Solución: Por la parte a(ii), al ser G abeliano, podemos buscar x e y con $\mathrm{mcd}(\mathrm{o}(x), \mathrm{o}(y)) = 1$ y $\mathrm{o}(x)\,\mathrm{o}(y) = 156 = \varphi(157)$. En ese caso tomando $g = xy$ tendríamos (por a(ii)) que $\mathrm{o}(g) = \mathrm{o}(x)\,\mathrm{o}(y) = 156$, y entonces g sería raíz primitiva módulo 157
Como $\mathrm{o}(2) = 52 = 13 \times 4$ y $\mathrm{o}(3) = 78 = 2 \times 39$, por la parte a(i) tenemos que $\mathrm{o}(2^{13}) = 4$ y $\mathrm{o}(3^2) = 39$ y como $\mathrm{mcd}(4, 39) = 1$ y $4 \times 39 = 156$ tomamos $x = 2^{13} \equiv 28$ e $y = 3^2 = 9$. Entonces $g = xy = 28 \times 9 \equiv 95 \pmod{157}$) es r.p. módulo 157

iv) ¿Cuántos homomorfismos $f : U(314) \to \mathbb{Z}_{15}$ hay?
Solución: Como $314 = 2(157)$ y 157 es primo, sabemos que existe g raíz primitiva módulo 314; es decir $U(314) = \langle g\rangle$ (y $\mathrm{o}(g) = 156$.)
Por lo tanto, los homomorfismo $F : U(314) \to \mathbb{Z}_{15}$ quedan determinados por $F(g) = k$ tal que $\mathrm{o}(k) \mid o(g)$ (y luego $F(g^n) = F(g)^n (= nk)$).
Es decir, que hay tantos homomorfismos como posibles $k \in \mathbb{Z}_{15}$ con $\mathrm{o}(k) \mid 156$. Como (por Lagrange) $\mathrm{o}(k) \mid |\mathbb{Z}_{15}| = 15$ buscamos los $k \in \mathbb{Z}_{15}$ tales que $\mathrm{o}(k) \mid \mathrm{mcd}(156, 15) = 3$. Los únicos k son $k = \overline{0}$ (de orden 1) y $k = \overline{5}$ o $k = \overline{10}$ (ambos de orden 3).
Entonces hay 3 homomorfismos.

Ejercicio 3.

a. Hallar todos los a, b enteros positivos tales que $a + b = 87$ y $\operatorname{mcd}(a, b) + \operatorname{mcm}(a, b) = 633$.
Solución: Sea $d = \operatorname{mcd}(a, b)$, como $d|a$ y $d|b$ entonces $d|87 = 3 \cdot 29$. Por otro lado, como $d|\operatorname{mcm}(a, b)$ entonces $d|633$ y $d|\operatorname{mcd}(87, 633) = 3$. Concluimos que $d \in \{1, 3\}$. También sabemos que $\operatorname{mcm}(a, b) \cdot \operatorname{mcd}(a, b) = |ab|$ y como buscamos a y b positivos tenemos que

$$ab + d^2 = d633.$$

Si $d = 1$: tenemos $ab = 632 = 2^3 79$ y $a + b = 87$. Como $d = 1$ entonces a y b son coprimos y vemos que las únicas opciones en este caso son $(a, b) = (8, 79)$ y $(a, b) = (79, 8)$.
Si $d = 3$: tenemos $ab + 9 = 3 \cdot 633$ y $ab = 3(633 - 3) = 3^2(211 - 1) = 2 \cdot 3^3 \cdot 5 \cdot 7$. Viendo las opciones posibles deducimos que las soluciones que nos sirven son $(a, b) = (45, 42)$, $(a, b) = (42, 45)$.

b. Enunciar y demostrar el Lema de Euclides.
Ver notas teóricas.

c. Hallar todos los a, b enteros tales que $ab + 3a = \frac{4b^2}{\operatorname{mcd}(a,b)} + 9b$.
Solución: Definimos $d = \operatorname{mcd}(a, b)$ y escribimos $a = d \cdot a^*$, $b = d \cdot b^*$, donde sabemos que $\operatorname{mcd}(a^*, b^*) = 1$. Por lo tanto $d^2 a^* b^* + 3da^* = 4d(b^*)^2 + 9db^*$, eliminando una d obtenemos

$$da^* b^* + 3a^* = 4(b^*)^2 + 9b^*.$$

Claramente b^* divide a el lado derecho de esa ecuación, por lo tanto $b^*|da^*b^* + 3a^*$ y $b^*|3a^*$. Como a^* y b^* son coprimos entonces por el Lema de Euclides deducimos que $b^*|3$, por lo que $b^* \in \{1, 3\}$.
Si $b^* = 1$: entonces $a^*(d + 3) = 13$ por lo que $a^* = 1$ o $a^* = 13$, ya que 13 es primo. Si $a^* = 1$ entonces $d = 10$, de donde obtenemos la solución $(a, b) = (10, 10)$. Si $a^* = 13$ entonces $d + 3 = 1$, que no puede pasar.
Si $b^* = 3$ entonces $a^*(d + 1) = 21$. Como antes $a^* = 1$, $a^* = 3$, $a^* = 7$ o $a^* = 21$. Si $a^* = 1$ entonces $d = 20$ y obtenemos la solución $(a, b) = (20, 60)$. No puede pasar $a^* = 3$ ya que tiene que ser coprimo con b^*. Si $a^* = 7$ entonces $d = 2$ y obtenemos la solución $(a, b) = (14, 6)$. No puede pasar $a^* = 21$ ya que tiene que ser coprimo con b^*.
Las soluciones entonces son

$$(10, 10),\ (20, 60),\ (14, 6).$$

Universidad de la República - Facultad de Ingeniería - IMERL.
Matemática Discreta 2

EXAMEN - 11 DE JULIO DE 2017. DURACIÓN: 3 HORAS Y MEDIA.

Ejercicio 1.

a. Enunciar y demostrar la Identidad de Bézout.

b. Deducir el Lema de Euclides.

c. Hallar todos los $x \in \mathbb{Z}$ que cumplan:

$$\begin{cases} 5x \equiv 1 & (\text{mód } 47) \\ x \equiv 21^{44} & (\text{mód } 19)\,. \end{cases}$$

Solución.

a. **Teorema.** Dados $a, b \in \mathbb{Z}$ con $(a, b) \neq (0, 0)$, existen $x, y \in \mathbb{Z}$ tales que $ax+by = \operatorname{mcd}(a, b)$.

Demostración. Sea $S = \{ax + by \ : \ x, y \in \mathbb{Z}\} \cap \mathbb{Z}^+$. Basta probar que $d = \operatorname{mcd}(a, b) \in S$.

Por definición $S \subseteq \mathbb{Z}^+$, además $S \neq \emptyset$ pues $a^2 + b^2 \in S$. Por el principio del buen orden S tiene un mínimo que llamamos s_0. Como $s_0 \in S$ podemos escribir $s_0 = ax_0 + by_0$.

Mostraremos que $s_0 = d$, probando ambas desigualdades. En primer lugar como $d \mid a$ y $d \mid b$ tenemos que $d \mid ax_0 + by_0 = s_0$. Concluimos que $d \leq s_0$.

Ahora veremos que s_0 divide a a y a b. Por el teorema de división entera existen $q, r \in \mathbb{Z}$ tales que $a = q\,s_0 + r$ con $0 \leq r < s_0$. Entonces $r = a - q\,s_0 = a - q\,(ax_0 + by_0) = a(1 - qx_0) + b(-qy_0)$. Si $r > 0$ tendríamos $r \in S$ con $r < s_0$ lo que contradice que s_0 es el mínimo. Entonces $r = 0$ y concluimos que $s_0 \mid a$.

De la misma forma se prueba que $s_0 \mid b$. Entonces s_0 es un divisor común de a y de b y concluimos que $s_0 \leq d$.

En resumen, $d = s_0 \in S$ lo que concluye la demostración. $\square$

b. **Teorema.** Sean $a, b, c \in \mathbb{Z}$ con $\operatorname{mcd}(a, b) = 1$. Si $a \mid bc$ entonces $a \mid c$.

Demostración. Por la identidad de Bézout existen $x, y \in \mathbb{Z}$ tales que $ax + by = 1$. Multiplicando por c obtenemos $acx+bcy = c$. Ahora $a \mid a$ y por hipótesis $a \mid bc$, concluimos que $a \mid a(cx) + bc(y) = c$. $\square$

c. Calculando el inverso de 5 módulo 47 encontramos que la primera ecuación equivale a $x \equiv 19 \pmod{47}$ (en efecto, $5 \cdot 19 - 2 \cdot 47 = 1$).

Para la segunda ecuación observamos que $21^{44} \equiv 2^{44} \pmod{19}$. Como 19 es primo y 2 no es múltiplo de 19 tenemos que $2^{18} \equiv 1 \pmod{19}$ (pequeño Teorema de Fermat) de modo que $2^{44} \equiv 2^8 \equiv 256 \equiv 9 \pmod{19}$.

Entonces el sistema es equivalente a

$$\begin{cases} x \equiv 19 & (\text{mód } 47) \\ x \equiv 9 & (\text{mód } 19)\,. \end{cases}$$

Por el Teorema Chino de los restos, el sistema tiene solución única módulo $19 \cdot 47 = 893$.

Como *ya sabemos* de la primer parte que $5 \cdot 19 \equiv 1 \pmod{47}$, es fácil ver que una solución es $x = 9 + 10 \cdot (19 \cdot 5) \equiv 66 \pmod{893}$.

En definitiva la solución es $\{66 + 893 \cdot k \ : \ k \in \mathbb{Z}\}$.

Ejercicio 2.

a. Sea G un grupo y $g \in G$ un elemento de orden finito.

i) Probar que si $k \in \mathbb{Z}$ entonces

$$\mathrm{o}\left(g^k\right) = \frac{\mathrm{o}(g)}{\mathrm{mcd}(o(g), k)}.$$

ii) Deducir que $\mathrm{o}\left(g^k\right) = \mathrm{o}(g)$ si y sólo si $\mathrm{mcd}(k, \mathrm{o}(g)) = 1$.

b. Sabiendo que el grupo $U(p)$ de invertibles módulo un primo p es cíclico, probar que existen $\varphi(p-1)$ raíces primitivas módulo p.

Solución.

a. i) Denotamos $n = o(g)$, $d = \mathrm{mcd}(n, k)$ y $m = o(g^k)$. Podemos escribir $n = d\,n'$ y $k = d\,k'$ siendo n' y k' enteros coprimos. Tenemos que probar que $m = n'$.

En primer lugar $(g^k)^{n'} = g^{k\,n'} = g^{d\,k'\,n'} = g^{n\,k'} = (g^n)^{k'} = e^{k'} = e$, entonces $m \mid n'$.

Por otro lado, $(g^k)^m = e$, entonces $g^{k\,m} = e$ y como $o(g) = n$ se sigue que $n \mid k\,m$. Dividiendo entre d en ambos lados tenemos que $n' \mid k'\,m$ y por el Lema de Euclides $n' \mid m$.

En conclusión, $m \mid n'$ y $n' \mid m$ por lo tanto $m = n'$.

ii) Es claro.

b. Como $U(p)$ es cíclico, existe un generador $g \in U(p)$. Como $o(g) = p - 1$ tenemos que $U(p) = \{g^1, g^2, \ldots, g^{p-1}\}$ siendo estos elementos todos distintos.

Por la parte anterior $o(g^k) = p-1$ si y sólo si $\mathrm{mcd}(k, p-1) = 1$, entonces las raices primitivas (elementos de orden $p-1$) están en biyección con $\{k = 1, 2, \ldots, p-1 \ :\ \mathrm{mcd}(k, p-1) = 1\}$ cuyo cardinal es $\varphi(p-1)$.

Ejercicio 3.

a. i) Probar que 103 es un número primo.

ii) Probar que $g = 5$ es una raíz primitiva módulo el primo $p = 103$.

iii) Sabiendo que $g^{102} \equiv 1752 \pmod{103^2}$, probar que g es una raíz primitiva módulo p^2.

iv) Probar que g es una raíz primitiva módulo p^k para cada $k > 2$.

b. i) Describir el método de intercambio de claves de Diffie-Hellman.

ii) Mostrar que en el método Diffie-Hellman ambos participantes llegan a la misma clave.

Solución.

a. i) Basta con verificar que no es múltiplo de 2, de 3, de 5, o de 7, ya que $11^2 = 121 > 103$.

ii) Como 103 es primo $\varphi(103) = 102 = 2 \cdot 3 \cdot 17$, y alcanza probar que $5^{51} \not\equiv 1 \pmod{103}$, que $5^{34} \not\equiv 1 \pmod{103}$, y que $5^6 \not\equiv 1 \pmod{103}$.

En efecto calculamos $5^2 \equiv 25$, $5^4 \equiv 7$, $5^8 \equiv 49$, $5^{16} \equiv 32$, $5^{32} \equiv -6$. Ahora tenemos que $5^6 \equiv 5^4 \cdot 5^2 \equiv 7 \cdot 25 \equiv 72 \not\equiv 1$, que $5^{34} \equiv 5^{32} \cdot 5^2 \equiv -6 \cdot 25 \equiv 56 \not\equiv 1$, y que $5^{51} \equiv 5^{34} \cdot 5^{16} \cdot 5 \equiv 56 \cdot 32 \cdot 5 \equiv -1 \not\equiv 1$

iii) Llamemos n al orden de g módulo 103^2. Como $g^n \equiv 1 \pmod{103^2}$ también $g^n \equiv 1 \pmod{103}$ y por la parte anterior tenemos que $102 \mid n$.

Por otra parte sabemos que $n \mid \varphi(103^2) = 102 \cdot 103$. Como 103 es primo las únicas posibilidades son $n = 102$ o $n = 102 \cdot 103$.

Como $g^{102} \not\equiv 1 \pmod{103^2}$, concluimos que $n = 102 \cdot 103$ y por lo tanto g es raíz primitiva módulo 103^2.

iv) Por Lema 4.1.12 enunciado en teórico, si g es raíz primitiva módulo p^2, donde p es un primo impar, entonces es raíz primitiva módulo p^k para todo k.

Si se quiere hacer explícitamente: llamando n_k al orden de g módulo p^k, procediendo como en la parte anterior se ve que $n_k = (p-1)\,p^i$ con $i \in \{0, \dots, k-1\}$.
Para finalizar, usando que $g^{p-1} \equiv 1752 \equiv 1 + 17\,p \pmod{p^2}$ se puede probar por inducción en $k \geq 2$ que $g^{(p-1)\,p^{k-2}} \equiv 1 + 17\,p^{k-1} \not\equiv 1 \pmod{p^k}$. Concluimos que $n_k \nmid (p-1)\,p^{k-2}$ y la única opción posible es $n_k = (p-1)\,p^{k-1}$.

b. i) Ana y Beto eligen un primo grande p y un elemento $g \in U(p)$ con orden grande (por ejemplo, una raiz primitiva).
Ana elige un entero secreto A y calcula $a \equiv g^A \pmod{p}$, enviándolo a Beto.
Beto elige un entero secreto B y calcula $b \equiv g^B \pmod{p}$, enviándolo a Ana.
Son públicos p, g, a, b, y secretos A (conocido por Ana) y B (conocido por Beto).
Ana calcula $k \equiv b^A \pmod{p}$ y Beto calcula $k' \equiv a^B \pmod{p}$.

ii) En efecto $k \equiv b^A \equiv (g^B)^A \equiv g^{BA} \equiv g^{AB} \equiv (g^A)^B \equiv a^B \equiv k'$.

Ejercicio 4.

a. Describir todos los elementos de $(U(15), \times)$ indicando su orden y cuál es su inverso.

b. Describir todos los homomorfismos de $(\mathbb{Z}_4, +)$ en $(U(15), \times)$.
Indicar cuáles son inyectivos.

c. i) Encontrar un homomorfismo inyectivo $f : (\mathbb{Z}_2, +) \to (U(15), \times)$ y un homomorfismo inyectivo $g : (\mathbb{Z}_4, +) \to (U(15), \times)$ tales que $\operatorname{Im}(f) \cap \operatorname{Im}(g) = \{1\}$.

ii) Probar que la función $h : (\mathbb{Z}_2 \times \mathbb{Z}_4, +) \to (U(15), \times)$ dada por

$$h(a, b) = f(a)\,g(b)$$

es un homomorfismo.

iii) ¿Es el homomorfismo h un isomorfismo?

Solución.

a. $U(15) = \{x = 1, \dots, 15 \ : \ \operatorname{mcd}(x, 15) = 1\} = \{1, 2, 4, 7, 8, 11, 13, 14\}$. Elevando al cuadrado encontramos que $4^2 \equiv 11^2 \equiv 14^2 \equiv 1 \pmod{15}$ y $\{4, 11, 14\}$ son todos elementos de orden 2. Además $2^2 \equiv 7^2 \equiv 8^2 \equiv 13^2 \equiv 4 \pmod{15}$, entonces $2^4 \equiv 7^4 \equiv 8^4 \equiv 13^2 \equiv 1 \pmod{15}$ y $\{2, 7, 8, 13\}$ son todos elementos de orden 4 (no pueden tener orden 3 por el Teorema de Lagrange). Finalmente 1 tiene orden 1.

b. Como $\mathbb{Z}_4$ es cíclico generado por 1 de orden 4, cualquier homomorfismo es de la forma $g(n) = x^n$ para algún $x \in U(15)$ con $o(x) \mid 4$. Esto último vale para cualquier $x \in U(15)$, entonces hay 8 homomorfismos $g : \mathbb{Z}_4 \to U(15)$, uno para cada posible x.

La imágen de $g(n) = x^n$ es el subgrupo $\langle x \rangle$ de $U(15)$. Para que g sea inyectivo, su imagen debe tener orden 4, es decir $o(x) = 4$. Entonces los homomorfismos inyectivos son los cuatro dados por $g(n) = x^n$ donde $x = 2, 7, 8, 13$.

c. i) Por ejemplo $f(n) = 11^n$ y $g(n) = 2^n$, ya que $\operatorname{Im}(f) = \{1, 11\}$ y $\operatorname{Im}(g) = \{1, 2, 4, 8\}$.

ii) Sean $(a, b) \in \mathbb{Z}_2 \times \mathbb{Z}_4$ y $(a', b') \in \mathbb{Z}_2 \times \mathbb{Z}_4$. Entonces $h(a + a', b + b') = 11^{a+a'} \cdot 2^{b+b'} = 11^a \cdot 11^{a'} \cdot 2^b \cdot 2^{b'} = (11^a \cdot 2^b) \cdot (11^{a'} \cdot 2^{b'}) = h(a, b) \cdot h(a', b')$.

iii) En efecto $\operatorname{Im}(h)$ contiene a $\operatorname{Im}(f)$ y a $\operatorname{Im}(g)$ entonces $|\operatorname{Im}(h)| \geq 5$ pero por el Teorema de Lagrange debe dividir a $|U(15)| = 8$. Entonces h es sobreyectiva, y como $|\mathbb{Z}_2 \times \mathbb{Z}_4| = 8 = |U(15)|$ se concluye que h es un isomorfismo.
Nota: también pueden calcularse explícitamente los 8 valores de h y verificar de manera directa que el núcleo es trivial.