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 $\mathrm{o}(x^a) = b$.
Solución: Alcanza con probar que $(x^a)^b = e$ y que si $(x^a)^c = e$ entonces $b|c$.
Veamos la primer afirmación: $(x^a)^b = x^{ab} = e$ ya que $\mathrm{o}(x) = ab$. Si $(x^a)^c = e$ 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 $\text{mcd}(a, b) + \text{mcm}(a, b) = 633$.
Solución: Sea $d = \text{mcd}(a, b)$, como $d|a$ y $d|b$ entonces $d|87 = 3 \cdot 29$. Por otro lado, como $d|\text{mcm}(a, b)$ entonces $d|633$ y $d|\text{mcd}(87, 633) = 3$. Concluimos que $d \in \{1, 3\}$. También sabemos que $\text{mcm}(a, b) \cdot \text{mcd}(a, b) = |ab|$ 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 $ab + 3a = \frac{4b^2}{\text{mcd}(a,b)} + 9b$.
Solución: Definimos $d = \text{mcd}(a, b)$ y escribimos $a = d \cdot a^*$, $b = d \cdot b^*$, donde sabemos que $\text{mcd}(a^*, b^*) = 1$. Por lo tanto $d^2a^*b^* + 3da^* = 4d(b^*)^2 + 9db^*$, 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 $ax+by = \text{mcd}(a, b)$.

Demostración. Sea $S = \{ax + by \ : \ x, y \in \mathbb{Z}\} \cap \mathbb{Z}^+$. Basta probar que $d = \text{mcd}(a, b) \in S$. 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 $\text{mcd}(a, b) = 1$. 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 $\mathrm{Im}(f) \cap \mathrm{Im}(g) = \{1\}$.

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. $U(15) = \{x = 1, \dots, 15 \;:\; \mathrm{mcd}(x, 15) = 1\} = \{1, 2, 4, 7, 8, 11, 13, 14\}$. 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 $\mathrm{Im}(f) = \{1, 11\}$ y $\mathrm{Im}(g) = \{1, 2, 4, 8\}$.

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 $\mathrm{Im}(h)$ contiene a $\mathrm{Im}(f)$ y a $\mathrm{Im}(g)$ entonces $|\,\mathrm{Im}(h)| \geq 5$ 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.

Solución del examen - 9 de febrero de 2017.

Ejercicio 1. Hallar el menor entero positivo congruente a:

$$7^{217^{38}} \pmod{34}.$$

Solución. Primero observamos que se trata del número $7^{(217^{38})}$ módulo 34. Como $\mathrm{mcd}(7,34)=1$, podemos aplicar el Teorema de Euler y proceder a reducir 217^{38} módulo $\varphi(34)=16$. Ya que $217\equiv 9 \pmod{16}$, consideramos $9^{38} \pmod{16}$. De nuevo, $\mathrm{mcd}(9,16)=1$, pues por el mismo Teorema consideramos: 38 módulo $\varphi(16)=8$. Tenemos que $38\equiv 6 \pmod 8$, pues volviendo para atrás y aplicando la tesis del Teorema de Euler tenemos primero: $9^{38}\equiv 9^6 = 81^3\equiv 1 \pmod{16}$, luego: $7^{(217^{38})}\equiv 7^{(9^{38})}\equiv 7^1 = 7 \pmod{34}$. Así que el número buscado es 7.

Ejercicio 2.

a. ¿Qué es una ecuación diofántica?
Decidir cuándo tiene solución y qué forma tiene esta cuando existe. Probar ambas propiedades.

b. ¿Qué podemos decir sobre la existencia y el número de soluciones de la ecuación de congruencia:

$$ax\equiv b \pmod{m}?$$

Justificar.

c. Hallar todas las soluciones (módulo 64) de la ecuación de congruencia:

$$28x\equiv 44 \pmod{64}.$$

Solución. Las partes **a.** (Definición 1.5.2 y Teorema 1.5.3) y **b.** (Teorema 2.4.2) son de teórico, pero la prueba de la parte **b.** se basa en el resultado de la parte **a.**, con lo cual para la prueba de la parte **b.** basta mostrar la conexión que tiene con las ecuaciones diofánticas e interpretar el resultado sobre las soluciones.

c. Dado que $\mathrm{mcd}(28,64)=4|44$, existen exactamente 4 soluciones módulo 64. Dividiendo toda la ecuación entre 4 y aplicando la regla del teórico obtenemos que es equivalente a la ecuación $7x\equiv 11 \pmod{16}$. Esto nos lleva a la ecuación diofántica $7x-16y=11$. Resolviéndola llegamos a que $-3\cdot 16+7\cdot 7=1$, luego $16(-33)+7(77)=11$, de donde concluimos que una solución para x es 77. Para hallar el mínimo entero positivo x que es la solución, reducimos 77 módulo 16, obteniendo 13. Luego todas las soluciones de la ecuación de congruencia inicial módulo 64 son: $x=13+16k$ siendo $k=0,1,2,3$, esto es: $x\in\{13,29,45,61\}$.

Ejercicio 3. Hallar todas las soluciones en $\mathbb{Z}$ del sistema:

$$\begin{cases} 3x \equiv 10 \pmod{11} \\ 2x \equiv 7 \pmod{9} \\ x \equiv 8 \pmod{15} \\ 5x \equiv 10 \pmod{12} \\ x \equiv 18 \pmod{20}. \end{cases}$$

Solución. Para la primera, segunda y la cuarta ecuación buscamos primero los inversos de los coeficientes del lado izquierdo. Solucionando las tres ecuaciones de congruencia: $3x\equiv 1 \pmod{11}, 2x\equiv 1 \pmod 9, 5x\equiv 1 \pmod{12}$ obtenemos fácilmente que los inversos respectivos son: 4,5,5, respectivamente. De ahí, las tres ecuaciones de congruencia iniciales se reducen a: $x\equiv 40\equiv 7 \pmod{11}, x\equiv 35\equiv 8 \pmod 9$ y $x\equiv 50\equiv 2 \pmod{12}$. Con eso el sistema inicial es equivalente a:

$$\begin{cases} x \equiv 7 \pmod{11} \\ x \equiv 8 \pmod{9} \\ x \equiv 8 \pmod{15} \\ x \equiv 2 \pmod{12} \\ x \equiv 18 \pmod{20} \end{cases}$$

Tenemos entonces las siguientes implicaciones y equivalencias:

$$\begin{cases} x \equiv 7 \pmod{11} & \\ x \equiv 8 \pmod{9} & \Rightarrow x \equiv 2 \pmod{3} \\ x \equiv 8 \pmod{15} & \Leftrightarrow (x \equiv 3 \pmod{5} \quad \text{y} \quad x \equiv 2 \pmod{3}) \\ x \equiv 2 \pmod{12} & \Leftrightarrow (x \equiv 2 \pmod{4} \quad \text{y} \quad x \equiv 2 \pmod{3}) \\ x \equiv 18 \pmod{20} & \Leftrightarrow (x \equiv 3 \pmod{5} \quad \text{y} \quad x \equiv 2 \pmod{4}) \end{cases}$$

luego a la primera y la segunda ecuación las debemos preservar intactas y de las restantes es suficiente tomar las ecuaciones $x \equiv 3 \pmod{5}$ y $x \equiv 2 \pmod{4}$, o, lo que es lo mismo, la última ecuación de las de arriba. Así nos queda el sistema equivalente:

$$\begin{cases} x \equiv 7 \pmod{11} \\ x \equiv 8 \pmod{9} \\ x \equiv 18 \pmod{20}. \end{cases}$$

Resolviendo obtenemos: $x = 18 + 20k \equiv 7 \pmod{11}$ reduciendo: $9k \equiv 0 \pmod{11}$ de donde k debe ser un múltiplo de 11. Luego tenemos: $x = 18 + 20 \cdot 11s \equiv 8 \pmod{9}$, reduciendo: $4s \equiv 8 \pmod{9}$, luego $s \equiv 2 \pmod{9}$, ya que 4 es invertible módulo 9, pues $\operatorname{mcd}(4, 9) = 1$. Recolectando: $x = 18 + 20 \cdot 11(2 + 9p) = 458 + 20 \cdot 11 \cdot 9p$, para todo $p \in \mathbb{Z}$. Dicho de otro modo: $x \equiv 458 \pmod{20 \cdot 11 \cdot 9}$, la solución buscada.

Ejercicio 4.

a. Describir el método de Diffie - Hellman para acuerdo de clave.

b. Donald y Mickey, para garantizar la seguridad del gobierno de su país, se ponen de acuerdo en utilizar Diffie - Hellman y fijan el primo $p = 73$ y $g = 11$. Donald elige el número secreto $n = 71$ y Mickey le envía $g^m = 23$. ¿Cuál es la clave secreta que acuerdan Donald y Mickey?

c. Asignamos valores a algunos caracteres según la tabla siguiente:

A	B	C	D	E	J	L	M	N	O	P	S	R
0	1	2	3	4	5	6	7	8	9	10	11	12

Definimos el criptosistema afín de la siguiente manera: para $a, b \in \mathbb{Z}$, con $1 \leq a \leq 12$, y $0 \leq b \leq 12$, consideramos la función de encriptado $E : \mathbb{Z}_{13} \to \mathbb{Z}_{13}$ tal que $E(x) = ax+b \pmod{13}$. Sea $0 \leq W < 73$ la clave acordada por Donald y Mickey. Escribamos $W = a \cdot 13 + b$ con $0 \leq a < 13$ y $0 \leq b < 13$. El encriptado se hace letra a letra usando la función E definida arriba. Encriptar la palabra DJNP.

d. Supongamos que somos espías rusos y que Donald le envió a Mickey un mensaje encripado según el criptosistema anterior (desconociendo los valores de a y b de la función de encriptado). Espías ayudantes han descubierto que el mensaje original (sin encriptar) tiene como segunda letra A y como cuarta letra E. El mensaje encriptado es $OCEJM$.

i) Hallar la función de encriptado (o sea hallar los valores de a y b) que usan Donald y Mickey.

ii) Desencriptar el mensaje $OCEJM$.

Solución.

a. Ver Sección **5.2.1** de las notas de teórico.

b. Queremos calcular $23^{71} \pmod{73}$. Por el teorema de Fermat tenemos que $23^{72} \equiv 1 \pmod{73}$, por lo tanto $23^{71} \cdot 23 \equiv 1 \pmod{73}$. O sea que 23^{71} es el inverso de 23 módulo 73 (o sea: $23^{71} \equiv (23)^{-1} \pmod{73}$). Necesitaríamos resolver la ecuación diofántica lineal: $23 \cdot x + 73 \cdot y = 1$. Usando el algoritmo de Euclides extendido obtenemos que el inverso es $x = 54$. O sea $23^{71} \equiv 54 \pmod{73}$.

c. Como $54 = 4 \cdot 13 + 2$ (de forma única, pues estamos escribiendo en base 13), entonces $a = 4$ y $b = 2$. La palabra encriptada es BOND.

d. i) Usando que A se transforma en C y que E se transforma en J podemos deducir que $a = 4$ y $b = 2$.
d. ii) Con el $a = 4$ y el $b = 2$ hallado arriba, se tiene que el mensaje desencriptado es JAMES.

Ejercicio 5.

a. Sea p un primo y k un entero positivo. Si g es un número par y raíz primitiva de p^k, probar que $g+p^k$ es raíz primitiva de $2p^k$.

b. Hallar explícitamente todos los homomorfismos de $U(54)$ en el grupo dihedral D_{12}.

Solución. La parte **a.** es de teórico (Lema 4.1.13).
b. Dado que $54 = 2 \cdot 3^3$, por el Teorema 4.1.15, $n = 54 = 2 \cdot 3^3$, y por lo tanto el grupo $U(54)$ es cíclico, con lo cual para determinar un morfismo $f : U(54) \to D_{12}$ basta definir $f(g) = k$ donde $o(k)|o(g)$, siendo g un generador de $U(54)$. Para hallar un generador de $U(54)$, veremos que 2 es raíz primitiva módulo 27, luego por la parte **a.** tendremos $U(54) = \langle 2 + 3^3 \rangle = \langle 29 \rangle$.
Siendo $\varphi(27) = 18 = 2 \cdot 3^2$, para demostrar que 2 es raíz primitiva módulo 27, basta probar que 2^9 y 2^6 no son congruentes con 1 módulo 27. Calculamos que $2^6 \equiv 10 \neq 1$ y $2^9 \equiv -1 \neq 1$ módulo 27.

Ahora basta definir $f(29) = k$ de modo que $o(k)|18$. Los posibles órdenes de los elementos en D_{12}, por el Teorema de Lagrange, son 1, 2, 3, 4, 6, 8, 12 (son los divisores de $|D_{12}| = 24$, omitiendo el 24, ya que D_{12} no es cíclico, obsérvese que las simetrías tienen orden 2 y las potencias de la rotación mínima ρ tienen órdenes 3, 4 o 6). De estos posibles órdenes los que dividen a 18 son 1, 2, 3 y 6, luego las imágenes $f(29) = k$ pueden ser:

- la identidad;
- cualquiera de las 12 simetrías y la rotación ρ^6 (tienen orden 2);
- las rotaciones ρ^2 y ρ^{10} (de orden 6); y
- por último: ρ^4 y ρ^8 (de orden 3).

En total son 18 homomorfismos.

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

Examen - 14 de diciembre de 2016 Duración: 3 horas y media

Ejercicio 1.

a. Halle el menor entero positivo x tal que $\begin{cases} 5x - 3 \equiv 4 \pmod 7 \\ 4x + 2 \equiv 6 \pmod 9 \end{cases}$

Solución: La primera ecuación es equivalente a $5\,x \equiv 0 \pmod 7$, que tiene solución única módulo 7 pues $\mathrm{mcd}(5, 7) = 1$. Es claro que $x \equiv 0 \pmod 7$ es solución.

La segunda ecuación es equivalente a $4\,x \equiv 4 \pmod 9$, que tiene solución única módulo 9 pues $\mathrm{mcd}(4, 9) = 1$. Es claro que $x \equiv 1 \pmod 9$ es solución.

Como $\mathrm{mcd}(7, 9) = 1$, el sistema tiene solución única módulo $7 \cdot 9$. Se obtiene por el procedimiento estándar y es fácil verificar que $x \equiv 28 \pmod{63}$ satisface ambas ecuaciones.

El menor entero positivo es entonces $x = 28$.

b. Halle todas las parejas de enteros (a, b) tales que $a^2 + b^2 = 637$ y $\mathrm{mcd}(a, b) = \frac{x}{4}$ (x hallado en el ítem anterior).

Solución: Como $\mathrm{mcd}(a, b) = 7$, escribimos $a = 7\,a_0$ y $b = 7\,b_0$. Sustituyendo en la primera ecuación resulta $a_0^2 + b_0^2 = \frac{637}{49} = 13$.

Calculando $13 - i^2$ para $i = 0, \ldots, 3$ se determina que el único par de cuadrados que suman 13 es $4 + 9$. Considerando orden y signos encontramos ocho soluciones para (a_0, b_0), a saber: $\{(\pm 2, \pm 3), (\pm 3, \pm 2)\}$.

Multiplicando por 7 obtenemos las parejas pedidas:

$$(14, 21),\ (14, -21),\ (-14, 21),\ (-14, -21),\ (21, 14),\ (21, -14),\ (-21, 14),\ (-21, -14)$$

Ejercicio 2.

a. Calcular todas las raíces primitivas de U(31). ¿Cuántas son?

Solución: Como 31 es primo, $U(31)$ tiene 30 elementos y $\varphi(30) = 8$ raíces primitivas.

Como $2^5 \equiv 1 \pmod{31}$ sabemos que 2 no es raíz primitiva. Verificamos que $3^{30/2} \equiv 30 \not\equiv 1 \pmod{31}$, $3^{30/3} \equiv 25 \not\equiv 1 \pmod{31}$, $3^{30/5} \equiv 16 \not\equiv 1 \pmod{31}$, luego $g = 3$ es una raíz primitiva.

Sabemos que todas las raíces primitivas serán de la forma g^i donde $\mathrm{mcd}(i, 30) = 1$, es decir g, g^7, g^{11}, g^{13}, g^{17}, g^{19}, g^{23}, g^{29}.

Calculamos estas potencias módulo 31 obteniendo 3, 17, 13, 24, 22, 12, 11, 21.

b. Ordenar en forma creciente las raíces primitivas halladas en el ítem anterior: $r_1 < r_2 < r_3 < r_4 < \ldots$. Luego escribir la secuencia:

$$(r_1{+}r_4), (r_6{-}r_1), (r_5{-}r_4), (r_3), (r_2{-}r_1), (r_8{-}r_3{+}r_1), (r_7{-}r_1), (r_8{+}r_1), (r_5{+}r_1), (r_2{-}r_1), (r_5{+}r_3{-}r_1), (r_8{-}r_6{-}r_1).$$

Solución: $r_1 = 3$, $r_2 = 11$, $r_3 = 12$, $r_4 = 13$, $r_5 = 17$, $r_6 = 21$, $r_7 = 22$, $r_8 = 24$, y la secuencia es

$$16,\ 18,\ 4,\ 12,\ 8,\ 15,\ 19,\ 27,\ 20,\ 8,\ 26,\ 0.$$

c. Traducir la expresión anterior usando:

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

Solución: PREMIOS␣TIZA

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

$$VLMWSCLHFIYTJQPMLF\text{␣}MT$$

Solución: El texto cifrado corresponde a la secuencia

$$22,\ 11,\ 12,\ 23,\ 19,\ 2,\ 11,\ 7,\ 5,\ 8,\ 25,\ 20,\ 9,\ 7,\ 16,\ 12,\ 11,\ 5,\ 27,\ 12,\ 20.$$

Repetimos la expresión clave como la secuencia hallada en la parte b

$$16,\ 18,\ 4,\ 12,\ 8,\ 15,\ 19,\ 27,\ 20,\ 8,\ 26,\ 0,\ 16,\ 18,\ 4,\ 12,\ 8,\ 15,\ 19,\ 27,\ 20.$$

y restamos módulo 28 para obtener

$$6,\ 21,\ 8,\ 11,\ 11,\ 15,\ 20,\ 8,\ 13,\ 0,\ 27,\ 20,\ 21,\ 17,\ 12,\ 0,\ 3,\ 18,\ 8,\ 13,\ 0.$$

Traduciendo se obtiene el mensaje en claro

GUILLOTINA␣TU␣MADRINA

Ejercicio 3.

a. Enunciar y demostrar el Teorema de Lagrange para grupos finitos.

Solución: Ver Teorema 3.8.1 en la página 55 de las notas del curso.

b. Probar que todo grupo de orden p primo es cíclico.

Solución: Sea G un grupo de orden p primo, y sea $g \in G$ un elemento con $g \neq e$ (que siempre existe pues $p \geq 2$). El grupo $\langle g \rangle$ generado por g es un subgrupo de G no trivial (porque $g \neq e$).

Por el Teorema de Lagrange, el orden de $\langle g \rangle$ divide a p; como no es 1 debe ser p. Entonces $\langle g \rangle = G$ y g es un generador de G.

En las notas esto aparece como parte 3 del Corolario 3.8.2.

c. Sea G un grupo y sean G_1 y G_2 dos subgrupos *distintos* de orden p primo.
¿Qué puede decir sobre $G_1 \cap G_2$?

Solución: Como G_1 tiene orden primo y $G_1 \cap G_2$ es un subgrupo de G_1, con el mismo razonamiento que en la parte anterior se deduce que el orden de $G_1 \cap G_2$ es 1 o p. Si el orden de $G_1 \cap G_2$ fuera p debería ser igual a G_1, pero también debería ser igual a G_2, lo que contradice $G_1 \neq G_2$.

Entonces $G_1 \cap G_2$ es trivial.

EXAMEN - 20 DE JULIO DE 2016. ESQUEMA DE SOLUCIÓN

Ejercicio 1. Encontrar todos los n naturales tales que

$$\mathrm{mcd}(n, 143)^2 = n + 65.$$

Solución: Sea $d = \mathrm{mcd}(n, 143)$, como $143 = 11 \cdot 13$ tenemos que $d \in \{1, 11, 13, 143\}$. Vemos para que d hay algún n solución.

- Si $d = 1$ entonces $1 = n + 65$ y $n = 1 - 65 = -64 \notin \mathbb{N}$. Por lo que $d = 1$ queda descartado.
- Si $d = 11$ entonces $121 = n + 65$ y $n = 56 = 7 \cdot 8$, pero $\mathrm{mcd}(65, 143) = 1$ por lo que $d = 11$ queda descartado.
- Si $d = 13$ entonces $169 = n + 65$ y $n = 104 = 8 \cdot 13$ y $\mathrm{mcd}(104, 143) = 13$ por lo que $n = 104$ es solución.
- Si $d = 143$ entonces $143^2 = n + 65$ y $n = 143^2 - 65$. Como $11 \nmid 65$ entonces $11 \nmid n$ y queda descartado $d = 143$.

En resumen la única solución es $n = 104$.

Ejercicio 2. Calcular $0 \leq x < 245$ tal que

$$x \equiv 20^{465} \pmod{245}.$$

Solución: Como $245 = 5 \cdot 49$ la congruencia es equivalente a $\begin{cases} x \equiv 20^{465} \pmod{5} \\ x \equiv 20^{465} \pmod{49} \end{cases}$, por el Teorema Chino del Resto. Ahora, la primer congruencia del sistema es claramente equivalente a $x \equiv 0 \pmod{5}$ ya que $5 \mid 20$. Para la segunda podemos utilizar el Teorema de Euler. Primero vemos que $\varphi(49) = 7 \cdot 6 = 42$, y $465 = 42 \cdot 11 + 3$ por lo que $x \equiv 20^3 \pmod{49} \equiv 400 \cdot 20 \pmod{49} \equiv 8 \cdot 20 \pmod{49} \equiv 160 \pmod{49} \equiv 13 \pmod{49}$. Concluimos que el sistema original es equivalente a:

$$\begin{cases} x \equiv 0 \pmod{5} \\ x \equiv 13 \pmod{49} \end{cases}.$$

La solución al sistema anterior es 160, por lo que $x \equiv 160 \pmod{245}$.

Ejercicio 3. Para los siguientes sistemas investigar si tienen solución, y en caso afirmativo, hallar todas las soluciones en $\mathbb{Z}$.

a. $\begin{cases} x \equiv 23 \pmod{77} \\ x \equiv 67 \pmod{88} \\ x \equiv 2 \pmod{49} \\ x \equiv 23 \pmod{28} \end{cases}$. **b.** $\begin{cases} x \equiv 29 \pmod{77} \\ x \equiv 7 \pmod{88} \\ x \equiv 40 \pmod{49} \\ x \equiv 23 \pmod{28} \end{cases}$.

Solución:

a. Separando los módulos de las congruencias en producto de coprimos vemos que el sistema es equivalente a

$$\begin{cases} x \equiv 23 \pmod{7} \\ x \equiv 23 \pmod{11} \\ x \equiv 67 \pmod{8} \\ x \equiv 67 \pmod{11} \\ x \equiv 2 \pmod{49} \\ x \equiv 23 \pmod{4} \\ x \equiv 23 \pmod{7} \end{cases} \Leftrightarrow \begin{cases} x \equiv 2 \pmod{7} \\ x \equiv 1 \pmod{11} \\ x \equiv 3 \pmod{8} \\ x \equiv 1 \pmod{11} \\ x \equiv 2 \pmod{49} \\ x \equiv 3 \pmod{4} \\ x \equiv 2 \pmod{7} \end{cases}.$$

Eliminando las repeticiones y las implicancias de potencias de los módulos llegamos al sistema equivalente:

$$\begin{cases} x \equiv 1 \pmod{11} \\ x \equiv 3 \pmod{8} \\ x \equiv 2 \pmod{49} \end{cases}.$$

Utilizando el método de resolución de sistemas vemos que tiene solución $x \equiv 2795 \pmod{8 \cdot 11 \cdot 49}$, y todas las soluciones son $x = 2795 + 4312 \cdot k$ con $k \in \mathbb{Z}$.

b. De igual manera al sistema anterior, obtenemos que el sistema es equivalente a:

$$\begin{cases} x \equiv 29 \pmod 7 \\ x \equiv 29 \pmod{11} \\ x \equiv 7 \pmod 8 \\ x \equiv 7 \pmod{11} \\ x \equiv 40 \pmod{49} \\ x \equiv 23 \pmod 4 \\ x \equiv 23 \pmod 7 \end{cases} \Leftrightarrow \begin{cases} x \equiv 1 \pmod 7 \\ x \equiv 7 \pmod{11} \\ x \equiv 7 \pmod 8 \\ x \equiv 7 \pmod{11} \\ x \equiv 40 \pmod{49} \\ x \equiv 3 \pmod 4 \\ x \equiv 2 \pmod 7 \end{cases}.$$

El sistema anterior no tiene solución ya que si $x \equiv 40 \pmod{49}$ entonces $x \equiv 5 \pmod 7$ que es incongruente con la primer congruencia $x \equiv 1 \pmod 7$.

Ejercicio 4.

a. Sea $n > 1$ entero, probar que existe un primo p tal que $p \mid n$.

b. Probar que existen infinitos primos.

c. Enunciar y demostrar el Lema de Euclides.

Solución: Ver teórico.

Ejercicio 5.

a. Enunciar y demostrar el Teorema de Lagrange.

Solución: Ver teórico.

b. Sea el grupo $G = \mathbb{Z}_{14}$.

i) Listar los elementos de G junto a sus ordenes.
Solución:

g	o(g)
0	1
1	14
2	7
3	14
4	7
5	14
6	7
7	2
8	7
9	14
10	7
11	14
12	7
13	14

Observar que el orden se puede calcular usando la fórmula $\mathrm{o}(g^n) = \frac{\mathrm{o}(g)}{\mathrm{mcd}(n, \mathrm{o}(g))}$, y tomando $g = 1$ obtenemos que $\mathrm{o}(n) = \frac{14}{\mathrm{mcd}(14, n)}$.

ii) Listar todos los subgrupos de G.
Solución: Observamos que G es cíclico, y por lo tanto cualquier subgrupo de G es cíclico. Vemos entonces que los subgrupos H de G tienen que ser:

- $H = \{0\} = \langle 0 \rangle$.
- $H = G = \langle 1 \rangle = \langle 3 \rangle = \langle 5 \rangle = \langle 9 \rangle = \langle 11 \rangle$.
- $H = \{0, 2, 4, 6, 8, 10, 12\} = \langle 2 \rangle = \langle 4 \rangle = \langle 6 \rangle = \langle 8 \rangle = \langle 10 \rangle = \langle 12 \rangle$.
- $H = \{0, 7\} = \langle 7 \rangle$.
- $H = \{0, 13\} = \langle 13 \rangle$.

SOLUCIÓN DEL EXAMEN - 17 DE FEBRERO DE 2016.

Ejercicio 1.

a. Dados p, q, n, d y e en las hipótesis del criptosistema RSA y las funciones de cifrado $E(x) = x^e \pmod{n}$ y descifrado $D(y) = y^d \pmod{n}$. Probar que la función de descifrado funciona como tal; es decir, probar que:

$$D(E(x)) = x \pmod{n}\ \forall x \in \mathbb{Z}_n.$$

b. Dados los primos $p = 17$, $q = 19$ y $e = 11$, calcular la función de descifrado D.

c. Con los mismos datos que en (**b**) cifrar $x = 170$.

Solución:

a. Ver notas teóricas (Proposición 5.3.1 de los apuntes de teórico).

b. $n = pq = 17(19) = 323$; $\varphi(n) = 16(18) = 288$. La función de descifrado es $D(y) = y^d \pmod{n}$ siendo d tal que $ed \equiv 1 \pmod{\varphi(n)}$. Buscamos entonces d tal que $11d \equiv 1 \pmod{288}$. Realizando el algoritmo de Euclides extendido para 288 y 11 obtenemos que $11(131) - 5(288) = 1$ y por lo tanto $11(131) \equiv 1 \pmod{288}$ y entonces $d = 131$.

c. Debemos calcular $y = E(170) = 170^{11} \pmod{323}$. Como 17 y 19 son coprimos, esto equivale a hallar y tal que

$$\begin{cases} y \equiv 170^{11} \pmod{17} \\ y \equiv 170^{11} \pmod{19}. \end{cases}$$

Es decir

$$\begin{cases} y \equiv 0 \pmod{17} \\ y \equiv (-1)^{11} \pmod{19} \equiv -1 \pmod{19}, \end{cases}$$

y por lo tanto $y = 170$; es decir $E(170) = 170$.

Ejercicio 2. Sea G un grupo y $g \in G$.

a. Probar que $\langle g \rangle := \{g^n : n \in \mathbb{Z}\}$ es un subgrupo de G.

b. Probar que $|\langle g \rangle| = \mathrm{o}(g)$

c. Si G es finito, probar que $g^{|G|} = e_G$.

Solución: Ver notas teóricas (Proposición 3.7.4, 3.7.9 y parte (2) del Corolario 3.8.2).

Ejercicio 3.

a. Hallar todas las soluciones módulo 61 de la ecuación $3x \equiv 10 \pmod{61}$.

b. Sea la ecuación

$$4x \equiv 20 \pmod{100}. \qquad (1)$$

i) Hallar todas las soluciones módulo 100 de la ecuación (1).

ii) Hallar todas sus soluciones módulo 50 y 25 de la ecuación (1).

iii) ¿Cuántas soluciones módulo 1000 tiene la ecuación (1)?

Solución:

a. $3x \equiv 10 \pmod{61} \Leftrightarrow \exists y \in \mathbb{Z} : 3x - 61y = 10$. Realizando el algoritmo de Euclides extendido obtenemos que $3(41) - 61(2) = 1$ y por lo tanto, $3(410) - 61(20) = 10$. Por el teorema de ecuaciones diofánticas, como $\mathrm{mcd}(3, 61) = 1$ tenemos que todas las soluciones de $3x - 61y = 10$ son $(x, y) = (410 + 61k, 20 + 3k)$, $k \in \mathbb{Z}$. Por lo tanto todas las solciones de la ecuación $3x \equiv 10 \pmod{61}$ son $x = 410 + 61k, k \in \mathbb{Z}$; es decir, hay una única solución módulo 61, $x \equiv 410 \pmod{61} \equiv 44 \pmod{61}$.

Otra forma de resolverlo es, como $\mathrm{mcd}(3, 61) = 1$, 3 es invertible módulo 61. Hallamos primero el inverso de 3 módulo 61: como $3(41) - 61(2) = 1$ resulta que $3(41) \equiv 1 \pmod{61}$ y por lo tanto $3^{-1} \equiv 41 \pmod{61}$. Entonces $3x \equiv 10 \pmod{61} \Leftrightarrow x \equiv 10(41) \pmod{61} \equiv 410 \pmod{61} \equiv 44 \pmod{61}$.

Otra forma, es notando que $10 \equiv -51 \pmod{61} \equiv 3(-17) \equiv 44 \pmod{61}$ y como $\mathrm{mcd}(3, 61) = 1$, podemos cancelar el 3 de la ecuación módulo 61. Es decir, $3x \equiv 10 \pmod{61} \Leftrightarrow 3x \equiv 3(-17) \pmod{61} \Leftrightarrow x \equiv (-17) \pmod{61} \equiv 44 \pmod{61}$.

b. Como $\text{mcd}(4, 100) = 4$ y $4 \mid 20$, el teorema de ecuaciones con congruencias (Teorema 2.4.2 de los apuntes) nos dice que la ecuación tienen solución y además que hay exactamente $\text{mcd}(4, 100) = 4$ soluciones distintas módulo 100. Como $\text{mcd}(4, 100) = 4 \neq 1$ no se puede cancelar el 4 en la ecuación módulo 100; la cancelativa que podemos aplicar es la que dice que si $c \mid n$ entonces $ca \equiv cb \pmod{n} \Leftrightarrow a \equiv b \pmod{\frac{n}{c}}$ (ítem 2 de la Proposición 2.2.4 de los apuntes). Por lo tanto, cancelando el 4 obtenemos

$$4x \equiv 20 \pmod{100} \Leftrightarrow x \equiv 5 \pmod{25} \Leftrightarrow x = 5 + 25k,\ k \in \mathbb{Z}.$$

i) Por lo dicho antes, hay 4 soluciones distintas módulo 100 y por la cuenta anterior tenemos que ellas son $x_1 = 5$, $x_2 = 5 + 25 = 30$, $x_3 = 5 + 2(25) = 55$ y $x_4 = 5 + 3(25) = 80$.

ii) Como vimos antes, la ecuación es equivalente a $x \equiv 5 \pmod{25}$ y por lo tanto $x = 5$ es la única solución módulo 25. Como las soluciones son $x = 5 + 25k$, $k \in \mathbb{Z}$ tenemos que o $x = 5 + 50k$ o $x = 30 + 50k$, $k \in \mathbb{Z}$; por lo tanto hay dos soluciones módulo 50, ellas son $x_1 = 5$ y $x_2 = 30$.

iii) Como $1000 = 25(40)$, y las soluciones son de la forma $x = 5 + 25k$, $k \in \mathbb{Z}$; las (40) soluciones obtenidas con $k = 0, 1, \cdots, 39$ no son congruentes entre sí módulo 1000 (ya que la diferencia entre cualquier par de ellas es menor que 1000), y además, cualquier otra solución será congruente con una de éstas módulo 1000. Pues si $x = 5 + 25k$ y $k = 40q + r$ con $r \in \{0, 1, \cdots, 39\}$ entonces $x = 5 + 25k = 5 + 25(40q + r) = 5 + 1000q + 25r \equiv 5 + 25r \pmod{1000}$. Por lo tanto hay exactamente 40 soluciones distintas módulo 1000.

Ejercicio 4.

a. Probar que 2 es raíz primitiva módulo 59.

b. Hallar el orden de 57 módulo 59.

c. Encontrar todos los homomorfismos $f : U(59) \to S_3$.

d. Hallar una raíz primitiva módulo 118.

Solución:

a. Como $\text{mcd}(2, 59) = 1$ y $\varphi(59) = 58 = 2 \times 29$, por la parte 3 (o 4) de la Proposición 4.1.4 de los apuntes, tenemos que 2 es raíz primitiva módulo 59 si y sólo si $2^2 \not\equiv 1 \pmod{59}$ y $2^{29} \not\equiv 1 \pmod{59}$.

Tenemos que $2^2 = 4 \not\equiv 1 \pmod{59}$ y que $2^4 = 16$, $2^8 = 16^2 = 256 \equiv 20 \pmod{59}$, $2^{16} \equiv 20^2 \pmod{59} \equiv 400 \pmod{59} \equiv 46 \pmod{59}$; por lo tanto $2^{29} = 2^{16}\, 2^8\, 2^4\, 2 \equiv 46 \times 20 \times 16 \times 2 \pmod{59} \equiv 58 \pmod{59} \equiv -1 \pmod{59} \not\equiv 1 \pmod{59}$. Por lo tanto 2 es raíz primitiva módulo 59.

b. Como $\mid U(59) \mid = 58 = 2 \times 29$ y para todo $g \in U(59)$, $o(g)$ divide a $\mid U(59) \mid$, tenemos que las posibilidades para $o(57)$ son $1, 2, 29$ y 58. Como $57 \not\equiv 1 \pmod{59}$ y $57^2 \equiv (-2)^2 \pmod{59} \equiv 4 \pmod{59} \not\equiv 1 \pmod{59}$, tenemos que $o(57) \neq 1, 2$.

Por otro lado, $57^{29} \equiv (-2)^{29} \pmod{59} \equiv (-1)^{29} 2^{29} \pmod{59} \equiv (-1)(-1) \pmod{59} \equiv 1 \pmod{59}$; por lo tanto, $o(57) = 29$.

c. Por la parte a) tenemos que $U(59)$ es cíclico y generado por 2. Por lo tanto, todo elemento de $U(59)$ es de la forma 2^k, y entonces para dar un homomorfismo $f : U(59) \to S_3$, basta con dar la imagen de 2; ya que luego $g(2^k) = f(2)^k$. Por la proposición 3.9.9, para que el homorfimo esté bien definido, basta con dar $f(2) \in S_3$ tal que $o(f(2)) \mid o(2)$; es decir $f(2)$ tal que $f(2) \mid 58$. Como los elementos de S_3 tienen orden $1, 2$ o 3, las posibilidades para $o(f(2))$ son 1 y 2. El único elemento de S_3 con orden 1, es el neutro $e = Id$; y los elementos de S_3 con orden 2 son $\tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, $\tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$, $\tau_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$. Entonces hay cuatro homomorfismos $f : U(59) \to S_3$; ellos son $f(2^k) = Id$, $f(2^k) = \tau_1^k$, $f(2^k) = \tau_2^k$ y $f(2^k) = \tau_3^k$.

d. Como $118 = 2 \times 59$, 59 es primo, 2 es raíz primitiva módulo 59 y 2 es par; por el Lema 4.1.13 tenemos que $2 + 59$ es raíz primitiva módulo 2×59; es decir que 61 es raíz primitiva módulo 118.

Examen - 16 de diciembre de 2015.

Ejercicio 1.

a. Sea la función φ de Euler y dos enteros m, $n > 1$ tales que $\operatorname{mcd}(m, n) = 1$. Probar que

$$\varphi(mn) = \varphi(m)\varphi(n).$$

b. Mostrar con un ejemplo que lo anterior es falso si $\operatorname{mcd}(m, n) \neq 1$.

c. Calcular $\varphi(297)$.

d. Reducir $629^{362} \pmod{297}$.

Solución:

a. Ver notas teóricas.

b. Tomando $n = m = 2$ vemos que $\operatorname{mcd}(m, n) = 2 \neq 1$ y $\varphi(4) = 2 \neq \varphi(2)\varphi(2) = 1$.

c. Vemos que $297 = 3^3 11$ por lo que $\varphi(297) = \varphi(3^3)\varphi(11) = 3^2(3-1)(11-1) = 180$.

d. Vemos que $629 = 35 + 297 \cdot 2$ por lo que $629^{362} \equiv 35^{362} \pmod{297}$. Como 35 es coprimo con 297 podemos aplicar el teorema de Euler. Sabiendo que $362 = 2 + 180 \cdot 2$, llegamos a que

$$629^{362} \equiv 35^{362} \pmod{297} \equiv 35^2 \pmod{297} \equiv 1225 \pmod{297} \equiv 37 \pmod{297}.$$

Ejercicio 2.

a. Sea G un grupo finito y $x, y \in G$ tales que $xy = yx$ y $\operatorname{mcd}(\operatorname{o}(x), \operatorname{o}(y)) = 1$. Probar que

$$\operatorname{o}(xy) = \operatorname{o}(x)\operatorname{o}(y).$$

b. Sea $G = U(47)$ y $g = 2 \in G$. Probar que $\operatorname{o}(g) = 23$.

c. Utilizando lo anterior encontrar una raíz primitiva módulo 47.

d. ¿El grupo $U(15)$ es cíclico? Justique su respuesta.

Solución:

a. Ver notas teóricas.

b. Como 47 es primo, $|G| = \varphi(47) = 46 = 2 \cdot 23$. Por el Teorema de Lagrange el orden de 2 puede ser $1, 2, 23, 46$. Veamos que es efectivamente 23.

El orden de 2 no es 2 ya que $2^2 = 4 \not\equiv 1 \pmod{47}$. Alcanza con ver que $2^{23} \equiv 1 \pmod{47}$. Sabemos que $2^{10} = 1024 \equiv 37 \pmod{47}$. Por lo tanto $2^{23} = (2^{10})^2 2^3 \equiv 37^2 8 \pmod{47} \equiv 6 \cdot 8 \pmod{47} \equiv 1 \pmod{47}$.

c. Viendo que $\operatorname{o}(-1) = 2$ y $\operatorname{o}(2) = 23$ son coprimos y estamos en un grupo abeliano, podemos concluir utilizando la parte a. que $\operatorname{o}(-2) = \operatorname{o}(2)\operatorname{o}(-1) = 23 \cdot 2 = 46 = |G|$. Por lo tanto -2 es raíz primitiva módulo 47.

d. Por el Teorema de la raíz primitiva sabemos que $U(p \cdot q)$ nunca es cíclico cuando p, q son dos primos impares distintos. Alternativamente se puede hallar los ordenes de los elementos de $U(15)$ y ver que ninguno tiene el orden de $U(15)$ que es $\varphi(15) = 8$.

A continuación vemos todos los ordenes: $\operatorname{o}(1) = 1$, $\operatorname{o}(2) = 4$, $\operatorname{o}(4) = 2$, $\operatorname{o}(7) = 4$, $\operatorname{o}(8) = 4$, $\operatorname{o}(11) = 2$, $\operatorname{o}(13) = 4$, $\operatorname{o}(14) = 2$.

Ejercicio 3.

a. Sean $n = 253$ y $e = 9$. Para los datos anteriores hallar la función de descifrado $D : \mathbb{Z}_n \to \mathbb{Z}_n$ definida por el protocolo RSA.

b. Reducir $22^{666} \pmod{253}$.

Solución:

a. El número $n = 253 = 11 \cdot 23$ por lo que $\varphi(n) = 10 \cdot 22 = 220$. La función de descifrado es $D(y) = y^d \pmod{n}$ donde $d \equiv e^{-1} \pmod{\varphi(n)}$, o sea $d \equiv 9^{-1} \pmod{220}$. Utilizando el Algoritmo de Euclides Extendido obtenemos que $d \equiv 49 \pmod{220}$. Concluimos que $D(y) = y^{49} \pmod{253}$.

b. Como $22 = 2 \cdot 11$ no es coprimo con 253 no podemos aplicar el Teorema de Euler. Pero si podemos aplicar el Teorema Chino del Resto para hallar dicha potencia. Sabemos que

$$x \equiv 22^{666} \pmod{253} \Leftrightarrow \left\{ \begin{array}{lcl} x & \equiv & 22^{666} \pmod{11} \\ x & \equiv & 22^{666} \pmod{23} \end{array} \right. \Leftrightarrow \left\{ \begin{array}{lcl} x & \equiv & 0 \pmod{11} \\ x & \equiv & (-1)^{666} \pmod{23} \end{array} \right. \Leftrightarrow$$

$$\Leftrightarrow \left\{ \begin{array}{lcl} x & \equiv & 0 \pmod{11} \\ x & \equiv & 1 \pmod{23} \end{array} \right. .$$

Resolviendo obtenemos que $x \equiv 231 \pmod{253}$.

Ejercicio 4.

a. **i)** Sean $n, m \in \mathbb{Z}$ tal que $n \mid m$ y $a, b \in \mathbb{Z}$. Probar que

$$a \equiv b \pmod{m} \Longrightarrow a \equiv b \pmod{n}.$$

ii) ¿Vale el recíproco de lo anterior? Justificar.

b. Para el siguiente sistema investigar si tiene solución, y en caso de que tenga solución, hallar todas sus soluciones:

$$\left\{ \begin{array}{lcl} x & \equiv & 17 \pmod{88} \\ x & \equiv & 83 \pmod{286} \end{array} \right. .$$

Solución:

a. **i)** Ver notas teóricas.

ii) Un contraejemplo de lo anterior es $n = 2$, $m = 4$ y $a = 1$, $b = 3$. Claramente $1 \equiv 3 \pmod{2}$ pero $1 \not\equiv 3 \pmod{4}$.

b. Como los módulos del sistema no son coprimos no podemos aplicar directamente el Teorema Chino del Resto. Pero podemos aplicarlo a cada una de las congruencias y obtener

$$x \equiv 17 \pmod{88} \Leftrightarrow \left\{ \begin{array}{lcl} x & \equiv & 17 \pmod{8} \\ x & \equiv & 17 \pmod{11} \end{array} \right. \Leftrightarrow \left\{ \begin{array}{lcl} x & \equiv & 1 \pmod{8} \\ x & \equiv & 6 \pmod{11} \end{array} \right. ,$$

$$x \equiv 83 \pmod{286} \Leftrightarrow \left\{ \begin{array}{lcl} x & \equiv & 83 \pmod{2} \\ x & \equiv & 83 \pmod{11} \\ x & \equiv & 83 \pmod{13} \end{array} \right. \Leftrightarrow \left\{ \begin{array}{lcl} x & \equiv & 1 \pmod{2} \\ x & \equiv & 6 \pmod{11} \\ x & \equiv & 5 \pmod{13} \end{array} \right. .$$

Uniendo toda esa información vemos que nuestro sistema con módulos no coprimos es equivalente a

$$\left\{ \begin{array}{lcl} x & \equiv & 17 \pmod{88} \\ x & \equiv & 83 \pmod{286} \end{array} \right. \Leftrightarrow \left\{ \begin{array}{lcl} x & \equiv & 1 \pmod{8} \\ x & \equiv & 6 \pmod{11} \\ x & \equiv & 5 \pmod{13} \end{array} \right. ,$$

ya que las congruencias son todas compatibles. Una solución al sistema anterior utilizando el algoritmo para resolver sistemas es $x \equiv 369 \pmod{8 \cdot 11 \cdot 13}$.

olución Examen - 22 de julio de 2015. Duración: 3:30 horas

Primera parte: Múltiple Opción

MO	
1	2

Ejercicio 1. Sean $n = 319$ y $e = 19$. 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. $D(y) = y^{42} \pmod{n}$.

B. $D(y) = y^{59} \pmod{n}$.

C. $D(y) = y^{84} \pmod{n}$.

D. $D(y) = y^{67} \pmod{n}$.

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 $319 = 11 \cdot 29$, por lo que $\varphi(11 \cdot 29) = 10 \cdot 28 = 280$. Utilizando el algoritmo extendido de Euclides obtenemos $d \equiv 59 \pmod{280}$.

Ejercicio 2. Sea $0 \leq m < 325$ tal que $m \equiv 435^{241} \pmod{325}$. Indicar cuál de las opciones es correcta:

A. $m = 65$.

B. $m = 110$.

C. $m = 300$.

D. $m = 175$.

Como $435 = 3 \cdot 5 \cdot 29$ no es coprimo con $325 = 5^2 \cdot 13$ no podemos aplicar el Teorema de Euler. Aplicando el Teorema Chino del Resto obtenemos

$$x \equiv 435^{241} \pmod{325} \Leftrightarrow \left\{ \begin{array}{lcl} x & \equiv & 435^{241} \pmod{5^2} \\ x & \equiv & 435^{241} \pmod{13} \end{array} \right. \Leftrightarrow \left\{ \begin{array}{lcl} x & \equiv & 5^{241}(3 \cdot 29)^{241} \pmod{5^2} \\ x & \equiv & 6^{241} \pmod{13} \end{array} \right. .$$

Ahora como $5^2 \mid 5^{241}$ entonces $435^{241} \equiv 0 \pmod{5^2}$. Por otro lado $\varphi(13) = 12$ y como 6 y 13 son coprimos, por el teorema de Euler tenemos que $6^{12} \equiv 1 \pmod{13}$, por lo que $6^{241} = 6^{12 \cdot 20 + 1} \equiv 6 \pmod{13}$. Concluímos que

$$x \equiv 435^{241} \pmod{325} \Leftrightarrow \left\{ \begin{array}{lcl} x & \equiv & 0 \pmod{5^2} \\ x & \equiv & 5 \pmod{13} \end{array} \right. ,$$

que tiene solución $x \equiv 175 \pmod{325}$. Por lo que $m = 175$.

Segunda parte: Desarrollo

Ejercicio 3. Dado los siguientes sistemas, investigar si tienen solución, y en caso que tenga encontrar todas sus respectivas soluciones.

a. $\left\{ \begin{array}{lcl} x & \equiv & 2 \pmod{11} \\ x & \equiv & 5 \pmod{8} \\ x & \equiv & 14 \pmod{15} \end{array} \right. .$

Como 11, 8 y 15 son coprimos dos a dos, por el Teorema Chino de Resto sabemos que existe solución y que es única módulo $11 \cdot 8 \cdot 15 = 1320$; es decir que existe una solución x_0 y todas las soluciones son $x \equiv x_0 \pmod{1320}$.

Si realizamos el cambio de variable $x' = x - 14$, el sistema en esta variable nos queda:

$$\left\{ \begin{array}{lclcl} x' & \equiv & -12 \pmod{11} & \equiv & -1 \pmod{11} \\ x' & \equiv & -9 \pmod{8} & \equiv & -1 \pmod{8} \\ x' & \equiv & 10 \pmod{15} & & \end{array} \right.$$

que equivale a $\left\{\begin{array}{lll} x' & \equiv & -1 \pmod{88} \\ x' & \equiv & 10 \pmod{15} \end{array}\right.$.

Es decir $x' = -1 + 88k$ con $k \in \mathbb{Z}$ y $-1 + 88k \equiv 0 \pmod{15}$. Entonces $13k \equiv 1 \pmod{15} \Rightarrow -2k \equiv 1 \pmod{15} \Rightarrow k \equiv 7 \pmod{15}$. Es decir $k = 7 + 15z : z \in \mathbb{Z}$. Entonces $x' = -1 + 88(7 + 15z) = 615 + 1320z$ y $x = x' + 14 = 629 + 1320z$, $z \in \mathbb{Z}$.

b. $\left\{\begin{array}{lll} x & \equiv & 9 \pmod{20} \\ x & \equiv & 5 \pmod{24} \\ x & \equiv & 35 \pmod{66} \end{array}\right.$.

Por el Teorema Chino del resto, tenemos que $x \equiv 9 \pmod{20}$ si y sólo si $\left\{\begin{array}{lllll} x & \equiv & 9 \pmod{4} & \equiv & 1 \pmod{4} \\ x & \equiv & 9 \pmod{5} & \equiv & 4 \pmod{5} \end{array}\right.$.

De forma análoga, tenemos que $x \equiv 5 \pmod{24}$ si y sólo si $\left\{\begin{array}{lllll} x & \equiv & 5 \pmod{8} & & \\ x & \equiv & 5 \pmod{3} & \equiv & 2 \pmod{3} \end{array}\right.$,

y que $x \equiv 35 \pmod{66}$ es equivalente a

$$\left\{\begin{array}{lllll} x & \equiv & 35 \pmod{2} & \equiv & 1 \pmod{2} \\ x & \equiv & 35 \pmod{3} & \equiv & 2 \pmod{3} \\ x & \equiv & 35 \pmod{11} & \equiv & 2 \pmod{11} \end{array}\right..$$

Entonces el sistema original es equivalente a

$$\left\{\begin{array}{lll} x & \equiv & 1 \pmod{4} \\ x & \equiv & 4 \pmod{5} \\ x & \equiv & 5 \pmod{8} \\ x & \equiv & 2 \pmod{3} \\ x & \equiv & 1 \pmod{2} \\ x & \equiv & 2 \pmod{11} \end{array}\right..$$

Ahora si $x \equiv 5 \pmod{8}$ entonces $x \equiv 5 \pmod{4} \equiv 1 \pmod{4}$ y $x \equiv 1 \pmod{2}$; por lo que la tercer ecuación implica la primera y la penúltima; y el sistema resulta equivalente a $\left\{\begin{array}{lll} x & \equiv & 4 \pmod{5} \\ x & \equiv & 5 \pmod{8} \\ x & \equiv & 2 \pmod{3} \\ x & \equiv & 2 \pmod{11} \end{array}\right.$.

Y como (por el Teo. Chino del Resto) $\left\{\begin{array}{lll} x & \equiv & 4 \pmod{5} \\ x & \equiv & 2 \pmod{3} \end{array}\right.$ equivale a $x \equiv 14 \pmod{15}$; obtenemos que el sistema original es equivalente al sistema $\left\{\begin{array}{lll} x & \equiv & 14 \pmod{15} \\ x & \equiv & 5 \pmod{8} \\ x & \equiv & 2 \pmod{11} \end{array}\right.$, que es el sistema resuelto en la parte anterior.

Ejercicio 4.

a. Definir la funcion $\varphi : \mathbb{N}^+ \to \mathbb{N}$ de Euler.

Ver teórico, definición 2.6.1.

b. Probar que si $\mathrm{mcd}(n, m) = 1$ entonces

$$\varphi(nm) = \varphi(n)\varphi(m).$$

Ver teórico Teorema 2.6.3.

c. Calcular:

i) $\varphi(125)$.

$$\varphi(125) = \varphi(5^3) = 5^3 - 5^2 = 100.$$

ii) $\varphi(108)$.

$\varphi(108) = \varphi(2^2 \cdot 3^3) = \varphi(2^2)\varphi(3^3) = (2^2 - 2)(3^3 - 3^2) = 2 \cdot 18 = 36$

d. Sabiendo que 2 es raíz primitiva módulo 25 y 125, hallar todos los homomofismos

$$f : U(125) \to U(25).$$

Como $U(125) = \langle \bar{2} \rangle$, por la proposición 3.9.9 de teórico, tenemos que todo morfismo $f : U(125) \to K$ es de la forma $f(\bar{2}^x) = f(\bar{2})^x$ con la condición de que $o(f(\bar{2})) \mid o(\bar{2})$. Ahora, como 2 es raíz primitiva módulo 125, el orden de $\bar{2}$ en $U(125)$ es $\varphi(125) = 100$. Entonces cada morfismo está determinado por la elección de $y = f(\bar{2}) \in U(25)$ tal que $o(y) \mid 100$. Ahora por el Corolario 3.8.2, tenemos que $o(y) \mid |U(25| = \varphi(25) = 20$ para todo $y \in U(25)$. Por lo que $o(y) \mid 100$ para todo $y \in U(25)$.

Entonces, existen tantos morfismos como elementos de $U(25)$. Es decir, hay 20 homomorfismos.

Ejercicio 5.

a. Sea G un grupo finito, y $g \in G$ tal que $\mathrm{o}(g) = m$. Probar que

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

Ver teórico (Proposición 3.7.8)

b. Probar que si existe una raíz primitiva módulo n entonces hay exactamente $\varphi(\varphi(n))$ raíces primitivas módulo n. Ver teórico (proposición 4.1.3)

c. Sea p un primo y g una raíz primitiva módulo p.

i) Probar que si n es el orden de g en $U(p^2)$ entonces $p - 1 \mid n$.
Si $n = \mathrm{o}(g)$ en $U(p^2)$, en particular $g^n \equiv 1 \pmod{p^2}$ es decir que $p^2 \mid g^n - 1$ y entonces $p \mid g^n - 1$. Por lo tanto $g^n \equiv 1 \pmod{p}$ y entonces si m es el orden de g en $U(p)$ tenemos que $m \mid n$.

ii) Probar que g o $g + p$ es raíz primitiva módulo p^2.
Por ser g raíz primitiva módulo p, sabemos que en $U(p)$ el orden de g es $p-1$. Por la parte anterior, tenemos que si n es el orden de g en $U(p^2)$ entonces $p - 1 \mid n$. Por otro lado, $n \mid |U(p^2)| = \varphi(p^2) = p(p - 1)$.
Por lo tanto, $p - 1 \mid n$ y $n \mid p(p - 1)$; al ser p primo tenemos que $n = p - 1$ o $n = p(p - 1)$. Si $n = p(p - 1)$ entonces g es raíz primitiva módulo p^2.
Veamos ahora qué pasa si $n = p - 1$. Llamemos m al orden de $g + p$ en $U(p^2)$. Tenemos entonces que $m \mid p(p - 1)$ y como $(g + p)^m \equiv 1 \pmod{p^2} \Rightarrow (g + p)^m \equiv 1 \pmod{p} \Rightarrow g^m \equiv 1 \pmod{p}$ tenemos que $p - 1 \mid m$. Es decir que $m = p - 1$ o $m = p(p - 1)$. Ahora

$$(g + p)^{p-1} = g^{p-1} + (p - 1)g^{p-2}p + \sum_{i=2}^{p-1} \binom{p-1}{i} g^{p-1-i}p^i \equiv g^{p-1} + (p - 1)g^{p-2}p \pmod{p^2}.$$

Como $n = p - 1$, tenemos que $g^{p-1} \equiv 1 \pmod{p^2}$ y entonces $(g + p)^{p-1} \equiv 1 + (p - 1)g^{p-2}p \pmod{p^2} \equiv 1 - g^{p-2}p \pmod{p^2}$. Como g es coprimo con p, $p \nmid g$ y entonces $p^2 \nmid g^{p-2}p$; por lo que $g^{p-2}p \not\equiv 0 \pmod{p^2}$ y entonces $(g + p)^{p-1} \not\equiv 1 \pmod{p^2}$. Concluímos entonces que $m \neq p - 1$, y entonces $m = p(p - 1)$ de lo que resulta que $g + p$ es raíz primitiva módulo p^2.

d. Hallar una raíz primitiva módulo 11^2.

Hallemos primero una raíz primitiva módulo 11. Como $\varphi(11) = 10 = 2 \times 5$, tenemos que g es raíz primitiva módulo 11, si y sólo si $\mathrm{mcd}(g, 11) = 1$ y $g^5 \not\equiv 1 \pmod{11}$ y $g^2 \not\equiv 1 \pmod{11}$.

Probando con $g = 2$, tenemos que $2^2 = 4 \not\equiv 1 \pmod{11}$ y que $2^5 = 32 \equiv 10 \pmod{11} \not\equiv 1 \pmod{11}$. Por lo tanto 2 es raíz primitiva módulo 11.

Por la parte anterior, tenemos que 2 o 13 es raíz primitiva módulo 11^2 y que los órdenes de estos elementos en $U(11^2)$ son 10 o $11 \cdot 10$. Como $2^{10} = 2^7 2^3 = 128 \cdot 8 \equiv 7 \cdot 8 \pmod{121} \equiv 56 \pmod{121} \not\equiv 1 \pmod{121}$, concluímos que el orden de 2 en $U(11^2)$ no es 10 y por lo tanto es $11 \cdot 10$. Y entonces 2 es raíz primitiva móculo 11^2.

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

Examen - 13 de febrero de 2015. Duración: 4 horas.

N° de examen	Cédula	Apellido y nombre

Ejercicio 1.

a. Probar que si $1 \leq n \leq 130$ y $n = a \cdot b$, con a, b naturales, entonces $a \leq 11$ o $b \leq 11$.

b. Listar todos los primos menores o iguales a 130, explicando brevemente el método utilizado.

c. Un coleccionista de discos tiene 3860 dolares que piensa gastar en discos. Los precios de los discos que le interesan de su tienda favorita son de 238 dolares y 178 dolares. ¿Cúantos discos puede comprar el coleccionista utilizando todo el dinero?

Ejercicio 2.

a. Hallar $x \equiv 79^{221} \pmod{81}$, con $0 \leq x < 81$.

b. Hallar el mínimo x positivo tal que $x \equiv 11^{181} \pmod{595}$.

Ejercicio 3.

a. Sea $n = 86$.

i) Hallar el orden de 9 módulo n, es decir el orden de $\overline{9} \in U(n)$.

ii) Hallar una raíz primitiva módulo n.

b. Amanda y Benito quieren pactar una clave común utilizando el protocolo Diffie-Hellman. Eligen el primo $p = 997$ y la raíz primitiva $g = 7$. Amanda elige el número $m = 504$ y le envía a Benito el número 994. Benito elige el número $n = 12$. ¿Cúal es la clave común que eligieron Amanda y Benito?

Ejercicio 4.

a. Enunciar y demostrar el teorema de Lagrange para grupos.

b. Sea G un grupo finito.

i) Probar que $\mathrm{o}(g) \mid |G|$ para todo $g \in G$.

ii) Probar que si $k \equiv l \pmod{|G|}$ entonces $g^k = g^l$ para todo $g \in G$.

iii) Sea $g \in G$ tal que $g^k = g^l$. Probar o refutar que $k \equiv l \pmod{|G|}$.

Examen - 13 de febrero de 2015.

Ejercicio 1.

a. Supongamos que $a > 11$ y $b > 11$, y como a y b son naturales $a \geq 12$, $b \geq 12$. Entonces

$$a \cdot b \geq 12 \cdot 12 = 144 > 130,$$

contradiciendo la hipotesis.

b. Por la parte anterior vemos que si $n \leq 130$ entonces sus divisores primos son menores o iguales a 11. Con lo anterior podemos utilizar la criba de Eratóstenes (ver teórico), eliminando los múltiplos de $2,\ 3,\ 5,\ 7,\ 11$ y vemos que los primos menores que 130 son:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127.$$

c. Tenemos que resolver la siguiente diofántica

$$3860 = 238x + 178y,$$

con $x,\ y$ enteros no negativos. La diofántica anterior tiene solución ya que $\operatorname{mcd}(238, 178) = 2 \mid 3860$. Aplicando el Algoritmo de Euclides Extendido vemos que

$$2 = 238 \cdot 3 + 178 \cdot (-4),$$

y multiplicando la ecuación por $\frac{3860}{2} = 1930$, obtenemos una solución particular de la diofántica

$$3860 = 238 \cdot (3 \cdot 1930) + 178 \cdot (-4 \cdot 1930) = 238 \cdot 5790 + 178 \cdot (-7720).$$

Con lo cual obtenemos la solución general de la diofántica

$$(x, y) = \left(5790 - \frac{178}{2} \cdot k, -7720 + \frac{238}{2} \cdot k\right) = (5790 - 89 \cdot k, -7720 + 119 \cdot k),\ k \in \mathbb{Z}.$$

Como queremos que $x,\ y \geq 0$, se tiene que cumplir que $5790 \geq 89 \cdot k$ y $119 \cdot k \geq 7720$, con lo cual

$$65{,}056... \geq k \geq 64{,}873... \ .$$

Concluimos que $k = 65$ y $(x, y) = (5, 15)$.

Ejercicio 2.

a. Primero calculamos $\varphi(81) = \varphi\left(3^4\right) = 2 \cdot 3^3 = 2 \cdot 27 = 54$. Como 79 y 81 son coprimos podemos utilizar el Teorema de Euler y obtenemos que

$$79^{221} \equiv (-2)^5 \pmod{81} \equiv -32 \pmod{81} \equiv 49 \pmod{81},$$

ya que $221 \equiv 5 \pmod{54}$.

b. Factorizamos $595 = 5 \cdot 7 \cdot 17$ y aplicamos el Teorema Chino del Resto para obtener la siguiente equivalencia

$$x \equiv 11^{181} \pmod{595} \Longleftrightarrow \begin{cases} x \equiv 11^{181} \pmod{5} \\ x \equiv 11^{181} \pmod{7} \\ x \equiv 11^{181} \pmod{17} \end{cases} \Longleftrightarrow \begin{cases} x \equiv 1 \pmod{5} \\ x \equiv 4 \pmod{7} \\ x \equiv 10 \pmod{17} \end{cases}.$$

Aplicando el Teorema Chino del Resto obtenemos que $x \equiv 571 \pmod{595}$.

Ejercicio 3.

a. Primero calculamos $\varphi(86) = \varphi(2 \cdot 43) = 42 = 2 \cdot 3 \cdot 7$.

i) Para hallar el orden de 9 alcanza con probar las potencias de 9 que dividen a 42. O sea que hay que probar con los $d \in \{1, 2, 3, 6, 7, 14, 21, 42\}$. Veamos cual es la primer potencia que es 1,

$$9^2 \equiv 81 \pmod{86}$$
$$9^3 \equiv 41 \pmod{86}$$
$$9^6 \equiv 47 \pmod{86}$$
$$9^7 \equiv 79 \pmod{86}$$
$$9^{14} \equiv 49 \pmod{86}$$
$$9^{21} \equiv 1 \pmod{86}$$

ii) Como $9 = 3^2$ y $o(9) = 21$, $2 \nmid 21$ entonces $o(3) = 42$.

b. Para hallar la clave tenemos que calcular $994^{12} \pmod{997} \equiv (-3)^{12} \pmod{997} \equiv 81^3 \pmod{997}$. Para calcular la potencia anterior vemos que $81^2 = 6561 = 6 \cdot 1000 + 561 = 6 \cdot (997 + 3) + 561 \equiv 6 \cdot 3 + 561 \pmod{997} \equiv 579 \pmod{997}$. Por último $81^3 \equiv 579 \cdot 81 \pmod{997} \equiv 46899 \pmod{997} \equiv 46 \cdot 3 + 899 \pmod{997} \equiv 40 \pmod{997}$.

Ejercicio 4.

a. Ver teórico.

b. i) Ver teórico.

ii) Ver teórico.

iii) La afirmación es falsa. Sea $G = U(12)$, con $|G| = \varphi(12) = 4$. Se cumple que si $\overline{(-1)} \in G$, entonces $\overline{(-1)}^1 = \overline{(-1)}^3$, pero $1 \not\equiv 3 \pmod{|G|}$.

Examen - 6 de diciembre de 2014.

Ejercicio 1.

a. Enunciar el Teorema Chino del Resto.

Ver notas de teórico.

b. Una señora va a la feria con una cesta con huevos. En un momento deposita la cesta en el piso y un joven en bicicleta se los rompe. El joven le ofrece pagarselos y le pregunta cuantos tenía. La señora no se acuerda, pero cuando los tomó de a 5 le sobraban 4, cuando los tomó de a 7 le sobraban 6, cuando los tomó de a 11 le sobraban 10 y cuando los tomó de a 13 no le sobro ninguno. ¿Cuál es la cantidad mínima de huevos que tenía la señora?

El sistema a resolver es:

$$\begin{cases} x \equiv 4 \pmod 5 \equiv -1 \pmod 5 \\ x \equiv 6 \pmod 7 \equiv -1 \pmod 7 \\ x \equiv 10 \pmod{11} \equiv -1 \pmod{11} \\ x \equiv 0 \pmod{13} \end{cases},$$

que tiene solución porque los módulos son todos primos. El sistema es equivalente a

$$\begin{cases} x \equiv -1 \pmod{5 \cdot 7 \cdot 11} \equiv -1 \pmod{385} \\ x \equiv 0 \pmod{13} \end{cases}.$$

La solución módulo $\operatorname{mcm}(13, 385) = 5005$ es $x = -1 + (5 \cdot 7 \cdot 11) \times \left((5 \cdot 7 \cdot 11)^{-1} \pmod{13}\right)$. Calculemos el inverso anterior:

$$(5 \cdot 7 \cdot 11)^{-1} \pmod{13} \equiv 8^{-1} \pmod{13} \equiv 5 \pmod{13}.$$

Entonces $x \equiv 385 \cdot 5 - 1 \pmod{5005} \equiv 1924 \pmod{5005}$.

c. Luego del incidente anterior, el mismo joven volvió a pisarle la cesta con huevos a otra señora, por lo cual el joven se compromete nuevamente a recompensarla. La señora conociendo la historia anterior le dice que cuando los tomó de a 10 le sobraron 5, cuando los tomó de a 12 le sobraron 7 y cuando los tomó de a 14 le sobro 2. Luego de meditarlo un momento, el joven increpa a la señora y le dice que eso no puede ser así. ¿Cuál de las dos partes tiene la razón?

El sistema a resolver es:

$$\begin{cases} x \equiv 5 \pmod{10} \\ x \equiv 7 \pmod{12} \\ x \equiv 2 \pmod{14} \end{cases}.$$

Observar que si x es solución del sistema, entonces $x \equiv 7 \pmod{12}$ y por lo tanto $x \equiv 7 \pmod 2 \equiv 1 \pmod 2$; es decir, x es impar. Por otro lado, $x \equiv 2 \pmod{14}$ entonces $x \equiv 2 \pmod 2 \equiv 0 \pmod 2$ y por lo tanto x es par. Concluímos entonces que el sistema no tiene solución por lo que el joven tiene razón.

Ejercicio 2.

a. Sea la función φ de Euler y dos enteros m, n tales $\operatorname{mcd}(m, n) = 1$, probar que

$$\varphi(mn) = \varphi(m)\varphi(n).$$

Ver notas de teórico.

b. Reducir $2^{1511} \pmod{1323}$.

Primero calculamos $\varphi(1323) = \varphi(3^3 \cdot 7^2) = 2 \cdot 3^2 \cdot 6 \cdot 7 = 756$. También vemos que $1511 \equiv 755 \pmod{756} \equiv -1 \pmod{756}$. Y por el teorema de Euler,

$$2^{1511} \equiv 2^{-1} \pmod{1323}.$$

Ahora, $1323 = 2 \cdot 662 - 1$ y $2^{-1} \equiv 662 \pmod{1323}$.

Ejercicio 3.

a. Sea un grupo finito G y $g \in G$, probar que si $k \in \mathbb{Z}^+$, entonces $o(g^k) = \dfrac{o(g)}{\operatorname{mcd}(o(g), k)}$.

Ver notas de teórico.

b. Sea el primo $p = 29$.

i) Hallar el orden de 13 módulo p.
Por el teorema de Lagrange, $\mathrm{o}(13) \mid \varphi(29) = 28 = 2^2 \cdot 7$, por lo que $\mathrm{o}(13) \in \{1, 2, 4, 7, 14, 28\}$. Calculamos algunas potencias, $13^2 = 169 \equiv 24 \pmod{29} \equiv -5 \pmod{29}$, por lo que $\mathrm{o}(13) \neq 2$. $13^4 \equiv (-5)^2 \pmod{29} \equiv 25 \pmod{29} \equiv -4 \pmod{29}$ y $\mathrm{o}(13) \neq 4$. $13^7 \equiv 13^{1+2+4} \pmod{29} \equiv 13 \cdot (-5) \cdot (-4) \pmod{29} \equiv 260 \pmod{29} \equiv -1 \pmod{29}$, por lo que $\mathrm{o}(13) \neq 7$. Por último, $13^{14} \equiv (-1)^2 \pmod{29} \equiv 1 \pmod{29}$, y $\mathrm{o}(13) = 14$.

ii) Probar que 10 es raíz primitiva módulo p.
Observar que $10^2 \equiv 100 \pmod{29} \equiv 13 \pmod{29}$. Utilizando la formula de la primer parte del ejercicio, con $g = 10$ y $k = 2$, vemos que

$$\mathrm{o}(13)\operatorname{mcd}(\mathrm{o}(10), 2) = \mathrm{o}(10).$$

Como antes, $\mathrm{o}(10) \in \{1, 2, 4, 7, 14, 28\}$. Si $\mathrm{o}(10) = 7$, entonces $14 = \mathrm{o}(13) = \mathrm{o}(13)\operatorname{mcd}(\mathrm{o}(10), 2) = \mathrm{o}(10) = 7$ lo cual es absurdo. Todas las otras posibilidades para el orden, que no sean 1, nos da que $\operatorname{mcd}(\mathrm{o}(10), 2) = 2$ y vemos que $o(10) = 28$, por lo cual es raíz primitiva.

iii) Hallar todos los $k \in \mathbb{Z}$ tales que $10^k \equiv 20 \pmod{p}$.
Por las partes anteriores, $20 = (-5) \cdot (-4) \equiv 13^2 13^4 \pmod{29} \equiv 10^4 10^8 \pmod{29} \equiv 10^{12} \pmod{29}$. Por lo tanto $k_0 = 12$ es solución. Ahora $10^k \equiv 20 \pmod{29}$ si y sólo si $10^k \equiv 10^{12} \pmod{29}$; si y sólo si $10^{k-12} \equiv 1 \pmod{29}$. Y como 10 es raíz primitiva módulo 29, esto sucede si y sólo si $28 \mid k - 12$. Es decir, si y sólo si $k \equiv 12 \pmod{28}$.

Ejercicio 4.

a. Probar que la función de desencriptado D en el protocolo RSA desencripta correctamente.

Ver notas de teórico.

b. Sean $n = 91$ y $e = 5$.

i) Hallar la función de descifrado D para el protocolo RSA.
Calculemos $\varphi(91) = \varphi(7 \cdot 13) = 6 \cdot 12 = 72$ y $5^{-1} \equiv 29 \pmod{72}$. Por lo cual $D(y) = y^{29} \pmod{91}$.

ii) Descifrar $y = 11$.
$11^{29} \equiv 72 \pmod{91}$

Examen - 24 de julio de 2014. Duración: 3 horas.

N° de examen	Cédula	Apellido y nombre

Ejercicio 1.

a. Sean $a, b \in \mathbb{Z}$ enteros no nulos. Probar que:

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

b. Hallar todos los a, b enteros positivos que cumplen $a \equiv 4 \pmod{b}$ y $\operatorname{mcm}(a,b) = 675 \times \operatorname{mcd}(a,b)$.

Ejercicio 2.

a. Hallar todas las soluciones $x \in \mathbb{Z}$ del siguiente sistema:

$$\begin{cases} x \equiv 1 \pmod{13} \\ x \equiv 4 \pmod{6} \\ x \equiv 0 \pmod{11} \end{cases}$$

b. Hallar el resto de dividir 22^{300} entre 4290.

Ejercicio 3.

a. Probar que si $f : G \to K$ es un homomorfismo de grupos y G es un grupo finito, entonces $|G| = |\ker(f)||\operatorname{Im}(f)|$. Si utiliza algún teorema de grupos, debe probarlo.

b. Probar que si G y K son grupos y $f : G \to K$ es un homomorfismo de grupos, entonces $|\operatorname{Im}(f)|$ divide a $\operatorname{mcd}(|G|, |K|)$.

c. Hallar todos los subgrupos del grupo dihedral D_3.

d.
- i) Sean p un primo impar y x un entero impar coprimo con p. Probar que x es raíz primitiva módulo p si y sólo si x es raíz primitiva módulo $2p$.
- ii) Probar que 11 es raíz primitiva módulo 82.
- iii) Hallar todos los homomorfismos $f : U(82) \to D_3$. *Sugerencia: utilizar las partes anteriores.*

Ejercicio 4. Sean $n = 209$ y $e = 17$.

a. Utilizando el método de cifrado RSA y la clave (n, e) cifrar $x = 5$.

b. Hallar $\varphi(n)$.

c. Hallar la función de descifrado D.

d. Descifrar $y = 10$.

Examen - 24 de julio de 2014.

Ejercicio 1.

a. Ver teórico.

b. Por letra $\text{mcd}(a, b) = \text{mcd}(4, a)$ por lo que, $\text{mcd}(a, b) = 1, 2$ o 4. Veamos caso por caso.

- Si $\text{mcd}(a, b) = 1$: se tiene que cumplir que $ab = 675 = 3^3 5^2$ y como son coprimos las posibilidades son:
  - $a = 1$, $b = 675$, que no cumple $a \equiv 4 \pmod{b}$.
  - $a = 25$, $b = 27$, que no cumple $a \equiv 4 \pmod{b}$.
  - $a = 27$, $b = 25$, que no cumple $a \equiv 4 \pmod{b}$.
  - $a = 675$, $b = 1$, que cumple las hipótesis.
- Si $\text{mcd}(a, b) = 2$: se cumple que $ab = 4 \times 675 = 2700 = 2^2 3^3 5^2$ y las posibilidades son:
  - $a = 2$, $b = 1350$, que no cumple $a \equiv 4 \pmod{b}$.
  - $a = 50$, $b = 54$, que no cumple $a \equiv 4 \pmod{b}$.
  - $a = 54$, $b = 50$, que cumple las hipótesis.
  - $a = 1350$, $b = 2$, que cumple las hipótesis.
- Si $\text{mcd}(a, b) = 4$: se cumple que $ab = 16 \times 675 = 10800 = 2^4 3^3 5^2$ y las posibilidades son:
  - $a = 4$, $b = 2700$, que cumple las hipótesis.
  - $a = 100$, $b = 108$, que no cumple $a \equiv 4 \pmod{b}$.
  - $a = 108$, $b = 100$, que no cumple $a \equiv 4 \pmod{b}$.
  - $a = 2700$, $b = 4$, que cumple las hipótesis.

En conclusión las soluciones son $a = 675$, $b = 1$, $a = 1350$, $b = 2$, $a = 4$, $b = 2700$, $a = 2700$, $b = 4$ y $a = 54$, $b = 50$.

Ejercicio 2.

a. La solución módulo $\text{mcm}(6, 11, 13) = 6 \cdot 11 \cdot 13 = 858$ es

$$\begin{aligned} x =& 4 \times (11 \cdot 13)^{-1} \pmod{6} \times (11 \cdot 13) + 0 \times (6 \cdot 13)^{-1} \pmod{11} \times (6 \cdot 13) \\ &+ 1 \times (6 \cdot 11)^{-1} \pmod{13} \times (6 \cdot 11) \\ =& 4 \times (11 \cdot 13)^{-1} \pmod{6} \times (11 \cdot 13) + 1 \times (6 \cdot 11)^{-1} \pmod{13} \times (6 \cdot 11). \end{aligned}$$

Hallemos los inversos involucrados,

$$\begin{aligned} &(11 \cdot 13)^{-1} \pmod{6} \equiv (-1)^{-1} \pmod{6} \equiv 5 \pmod{6}, \\ &(6 \cdot 11)^{-1} \pmod{13} \equiv 1^{-1} \pmod{13} \equiv 1 \pmod{13}. \end{aligned}$$

Por lo que $x = 2926 \equiv 352 \pmod{858}$.

b. Por el teorema chino del resto $x \equiv 22^{300} \pmod{4290}$ si y solo si

$$\begin{cases} x \equiv 22^{300} \pmod{5} \\ x \equiv 22^{300} \pmod{6} \\ x \equiv 22^{300} \pmod{11} \\ x \equiv 22^{300} \pmod{13} \end{cases} \text{si y solo si} \begin{cases} x \equiv 2^{0} \pmod{5} \\ x \equiv 4^{300} \pmod{6} \\ x \equiv 0^{300} \pmod{11} \\ x \equiv 9^{0} \pmod{13} \end{cases} \text{si y solo si} \begin{cases} x \equiv 1 \pmod{5} \\ x \equiv 4 \pmod{6} \\ x \equiv 0 \pmod{11} \\ x \equiv 1 \pmod{13} \end{cases}$$

y utilizando la parte anterior, el sistema es equivalente a

$$\begin{cases} x \equiv 1 \pmod{5} \\ x \equiv 352 \pmod{858} \end{cases}$$

Como $2 \times 858 - 343 \times 5 = 1$ entonces $x \equiv 352 \times (-343) \times 5 + 1 \times 2 \times 858 \pmod{4290} \equiv 2926 \pmod{4290}$

Ejercicio 3.

a. Ver teórico.

b. Ver teórico.

c. Sabemos que $D_3 = \{\mathrm{id}, s, sr, sr^2, r, r^2\}$ y $r^3 = \mathrm{id}$, $s^2 = \mathrm{id}$ y $rs = sr^2$. Por el teorema de Lagrange, sabemos que si H es un subgrupo de D_3 tiene que tener orden 1, 2, 3 o 6 ya que $|D_3| = 6$. Si un subgrupo tiene orden primo tiene que ser cíclico, por lo que los subgrupos de D_3 tienen que ser los generados por elementos del mismo y D_3. Veamos cuales son los subgrupos:

- $\{\mathrm{id}\}$.
- $\langle s\rangle = \{\mathrm{id}, s\}$.
- $(sr)^2 = srsr = ssr^2r = s^2r^3 = \mathrm{id}$, por lo que $\langle sr\rangle = \{\mathrm{id}, sr\}$.
- $(sr^2)^2 = sr^2sr^2 = rssr^2 = r^3 = \mathrm{id}$, por lo que $\langle sr^2\rangle = \{\mathrm{id}, sr^2\}$.
- $\langle r\rangle = \{\mathrm{id}, r, r^2\}$.
- D_3.

d. i) Como p es un primo impar tenemos que $\mathrm{mcd}(2, p) = 1$ y por lo tanto $\varphi(2p) = \varphi(p)$. Además, nuevamente como $\mathrm{mcd}(2, p) = 1$ podemos utilizar el teo. chino del resto y tenemos que $y^a \equiv 1 \pmod{2p}$ si y sólo si

$$\begin{cases} y^a \equiv 1 \pmod{2} \\ y^a \equiv 1 \pmod{p} \end{cases}$$

Por lo tanto, si x es impar, tenemos que x^a es impar y por lo tanto $x^a \equiv 1 \pmod{2}$. Entonces, si x es impar tenemos que $x^a \equiv 1 \pmod{2p}$ si y sólo si $x^a \equiv 1 \pmod{p}$. Y entonces $x^a \not\equiv 1 \pmod{2p}$ si y sólo si $x^a \not\equiv 1 \pmod{p}$.

Por otro lado, si x es impar y coprimo con p tenemos que x es raíz primitiva módulo $2p$ si y sólo si $x^a \not\equiv 1 \pmod{2p}$ para todo a divisor de $\varphi(2p) = \varphi(p)$, y por lo visto recién, ésto sucede si y sólo si $x^a \not\equiv 1 \pmod{p}$ para todo a divisor de $\varphi(p)$; es decir, si y sólo si x es raíz primitiva módulo p.

ii) Como 11 es impar, por la pate anterior, alcanza ver que es raíz primitiva módulo 41 ya que $82 = 2 \cdot 41$. Veamos eso: hay que probar que $11^{\frac{\varphi(41)}{p}} \not\equiv 1 \pmod{41}$ para $p = 2, 5$ ya que $\varphi(41) = 40 = 2^3 5$. Usando exponenciación rápida:

n	$11^{2^n} \pmod{41}$
0	11
1	$121 \equiv -2$
2	4
3	16
4	$256 \equiv 10$

Ahora $\frac{\varphi(41)}{2} = 2^2 5 = 20 = 2^3 + 2^1$ y $\frac{\varphi(41)}{5} = 8 = 2^3$, por lo que $11^{\frac{\varphi(41)}{2}} \equiv 10 \cdot (-2) \pmod{41} \equiv 21 \pmod{41}$, y $11^{\frac{\varphi(41)}{5}} \equiv 16 \pmod{41}$.

iii) Si $f : U(82) \to D_3$ homomorfismo de grupos y $g \in U(82)$ entonces $g = 11^n$ por lo que $f(g) = f(11)^n$, y alcanza con dar el valor de $f(11) \in D_3$ para describir f.

Por las partes anteriores $|\mathrm{Im}(f)|$ divide $\mathrm{mcd}(|U(82)|, |D_3|) = \mathrm{mcd}(40, 6) = 2$, y $|\mathrm{Im}(f)| = 1$ o 2. Vemos entonces que $\mathrm{o}(f(11)) = 1$ o 2, y $f(11) = \mathrm{id}, s, sr, sr^2$.

Ejercicio 4. Dados $n = 209$ y $e = 17$:

a. Para cifrar x debemos calcular $x^{17} \pmod{209}$, utilizamos exponenciación rápida:

n	$5^{2^n} \pmod{209}$
0	5
1	25
2	$625 \equiv -2$
3	4
4	16

Como $17 = 2^4 + 2^0$ entonces $5^{17} \equiv 5 \cdot 16 \pmod{209} \equiv 80 \pmod{209}$.

b. Descomponemos n, $209 = 11 \cdot 19$ y $\varphi(n) = 10 \cdot 18 = 180$.

c. Para encontrar la función de descifrado debemos hallar d el inverso de 17 módulo 180. Utilizando el algoritmo de Euclides extendido vemos que $d = 53$ y la funcion de descifrado es $D(y) = y^{53} \pmod{209}$.

Calculamos $D(10)$ usando exponenciación rápida:

n	$10^{2^n} \pmod{209}$
0	10
1	100
2	$10000 \equiv -32$
3	$1024 \equiv -21$
4	23
5	111

Ahora $53 = 2^5 + 2^4 + 2^2 + 2^0$ y $10^{53} \equiv 111 \cdot 23 \cdot (-32) \cdot 10 \pmod{209} \equiv 21 \pmod{209}$.

Hay otras formas de resolver esta parte, por ejemplo utilizando el teorema chino del resto. Tenemos que $x \equiv 10^{53} \pmod{209}$ si y sólo si

$$\begin{cases} x \equiv 10^{53} \pmod{11} \equiv (-1)^{53} \pmod{11} \equiv -1 \pmod{11} \\ x \equiv 10^{53} \pmod{19} \equiv 10^{3\times 18-1} \pmod{19} \equiv 10^{-1} \pmod{19} \equiv 2 \pmod{19} \end{cases}$$

Y resolviendo el sistema anterior resulta $x \equiv 21 \pmod{209}$.

Universidad de la República
Facultad de Ingeniería.

Solución Examen de Matemática Discreta II
17 de febrero de 2014

1. *a*) Sean a, b, n enteros positivos tales que $d = \text{mcd}(a, n)$, con $d \neq 1$ y $d \mid b$
Hallar todas las soluciones de $ax \equiv b$ mód (n). ¿Cuántas soluciones hay entre 1 y n?

   b) Resolver la ecuación diofántica $2x \equiv 14$ mód(80).

   c) Sea n el mayor natural mayor que 1 y menor que 80 que es solución de la ecuación de la parte anterior. Determinar cuántas raíces primitivas tiene $U(n)$, y hallar la menor de todas.

Resolución:

a) Como $d = mcd(a, n)$, entonces, consideramos, $a' = \frac{a}{d}$ y $n' = \frac{n}{d}$. Recordemos que mcd$(a', n') = 1$. Definimos también $b_0 = \frac{b}{d} \in \mathbb{Z}$, pues $d \mid b$. Tenemos que $ax \equiv b$ mód $(n) \Leftrightarrow$ existe $t \in \mathbb{Z}$ tal que $ax - b = tn$. Esto se cumple si y solo si existe $t \in \mathbb{Z}$ tal que $a'x - b_0 = tn'$ o sea si y solo si $a'x \equiv b_0$ mód(n'). Como mcd$(a', n') = 1$, existe el inverso de a' en U(n'), y por lo tanto la ecuación anterior es equivalente a: $x \equiv (a')^{-1}b_0$ mód(n'). O sea las soluciones de la ecuación inicial son de la forma: $x = (a')^{-1}b_0 + un'$, con $u \in \mathbb{Z}$.

El número de soluciones entre 1 y n las calculamos planteando: $1 \leq \alpha + un' \leq n = dn'$, siendo $\alpha = (a')^{-1}b_0$. La doble inecuación anterior es equivalente a: $\frac{1}{n'} - \frac{\alpha}{n'} \leq u \leq d - \frac{\alpha}{n'}$ con $u \in \mathbb{Z}$. Como $d - \frac{\alpha}{n'} - (\frac{1}{n'} - \frac{\alpha}{n'}) = d - \frac{1}{n'}$, en ese rango siempre encontramos d soluciones.

b) Por lo visto arriba las soluciones son $x = 7 + 40t$ con $t \in \mathbb{Z}$.

c) Entre 1 y 80 tenemos las soluciones 7 y 47. Entonces $n = 47$. Luego, $U(47)$ tiene, por lo visto en teórico, $\phi(\phi(47))$ raíces primitivas, siendo ϕ la función de Euler. Entonces $\phi(\phi(47)) = \phi(46) = \phi(2 \times 23) = \phi(23) = 22$. La menor raíz primitiva de 47 es 5, pues $2^{23} \equiv 1$ mód(47) y también $3^{23} \equiv 1$ mód(47) (por lo tanto 2 y 3 no son raíces primitivas) y por su parte $5^{23} \not\equiv 1$ mód(47) y $5^2 = 25 \not\equiv 1$ mód(47).

2. *a*) Sea $\sigma \in S_n$ y $\sigma = c_1 \dots c_n$ producto de ciclos disjuntos.
      1) Escribir $o(\sigma)$ en función de $o(c_1), \dots, o(c_n)$
      2) Probar el resultado enunciado en 1).

   b) Considerar $\mathbb{Z}_{30}$. Exhibir elementos $a, b \in \mathbb{Z}_{30}$ tales que $o(a + b) < \text{mcm}(o(a), o(b))$.

   c) Dado $(G, \cdot)$ grupo finito y $x, y \in G$ con $xy = yx$ entonces, si $a = o(x)$, $b = o(y)$, $m = mcm(a, b)$ y $d = mcd(a, b)$, demostrar que $\frac{m}{d} | o(xy)$ y que $o(xy) | m$.

Resolución:

a) 1) Se tiene que $o(\sigma) = \text{mcm}(o(c_1), \dots, o(c_n))$. O sea el orden de la permutación σ es el menor entero positivo que es múltiplo de todos los órdenes de los ciclos $c_1, c_2, ..., c_n$.

   2) Para demostrar la afirmación anterior llamemos $\beta = \text{mcm}(o(c_1), \dots, o(c_n))$. Tenemos que existen enteros positivos ν_i tal que $\beta = \nu_i \times o(c_i)$, para todo $i = 1, 2, ..., n$. Entonces $\sigma^\beta = (c_1 \dots c_n)^\beta = c_1^\beta . c_2^\beta . \cdots . c_n^\beta$, porque, al ser ciclos disjuntos, conmutan entre sí. Luego, cada $c_i^\beta = c_i^{\nu_i \times o(c_i)} = (c_i^{o(c_i)})^{\nu_i} = (id)^{\nu_i} = \text{id}$, para todo $i = 1, 2, ..., n$. Por lo tanto $\sigma^\beta = \text{id}$ y esto implica que o$(\sigma) \mid \beta$.

Por el otro lado, como $\sigma = c_1 \dots c_n$, se tiene que $(c_1 \dots c_n)^{o(\sigma)}$ =id. Como son ciclos disjuntos, conmutan entre sí, por lo que se obtiene: $c_i^{o(\sigma)} = c_1^{o(\sigma)}.c_2^{o(\sigma)}. \cdots .c_{i-1}^{o(\sigma)}.c_{i+1}^{o(\sigma)}. \cdots .c_n^{o(\sigma)}$. La igualdad anterior es posible si y solo si para todo $i = 1, ..., n$, $c_i^{o(\sigma)} = \mathrm{id} = c_1^{o(\sigma)}.c_2^{o(\sigma)}. \cdots .c_{i-1}^{o(\sigma)}.c_{i+1}^{o(\sigma)}. \cdots .c_n^{o(\sigma)}$ pues todos los ciclos son disjuntos. O sea que $\mathrm{o}(c_i) \mid \mathrm{o}(\sigma)$, para todo $i = 1, 2, ..., n$, por lo tanto $\beta = \mathrm{mcm}(o(c_1), \dots, o(c_n)) \mid \mathrm{o}(\sigma)$.

O sea, hemos probado que $\mathrm{o}(\sigma) = \beta$.

b) Es posible considerar muchas parejas que ejemplifiquen lo que se pide. Una pareja posible es: $a = 10$ y $b = 5$, pues $\mathrm{o}(10) = 3$, $\mathrm{o}(5) = 6$, mientras que $\mathrm{o}(10 + 5) = 2$.

c) Sean $a' = \frac{a}{d}$ y $b' = \frac{b}{d}$. Sabemos que m=mcm$(a, b) = ab' = a'b$. Consideramos $(xy)^m = x^m y^m$, pues x e y conmutan. Luego $(xy)^m = x^m y^m = (x^a)^{b'}(y^b)^{a'} = (id)^{b'}(id)^{a'} = id$. Por lo tanto $\mathrm{o}(xy) \mid m$.

Para abreviar llamemos t =o(xy). Entonces id $= (xy)^t = x^t y^t$, con lo que tenemos que $x^t = y^{-t}$. Luego $x^{ta} = (x^t)^a = (x^a)^t =$ id. Pero también: $x^{tb} = (x^t)^b = (y^{-t})^b = (y^b)^{-t} =$ id. Como $d = \mathrm{mcd}(a, b)$, por el Lema de Bezout, existen α y β enteros tales que $d = \alpha a + \beta b$. Entonces $x^{td} = x^{t(\alpha a + \beta b)} = (x^{ta})^\alpha (x^{tb})^\beta =$ id. O sea: $x^{td} =$ id. Por lo tanto $a = \mathrm{o}(x) \mid td$, o sea $a' \mid t$.

Análogamente se puede probar que $y^{td} =$ id con lo cual se concluye que $b = \mathrm{o}(y) \mid td$, o sea $b' \mid t$. Pero, recordemos que $\mathrm{mcd}(a', b') = 1$, por lo que $a'b' \mid t$. Conculyendo: $\frac{m}{d} = a'b' \mid \mathrm{o}(xy)$.

3. *a*) Calcular:
   - 41^{-1} mód(71);
   - 71^{-1} mód(41).

   b) Calcular 236^3 mód(2911) y 317^3 mód(2911).

   Sugerencia: usar el Teorema Chino del Resto.

   c) Sean $p = 41$, $q = 71$ y $n = p.q$.
   - ¿El par $(2911, 3)$ sirve como clave pública para *RSA*? Justifique.
   - Se usa *Cifrado en Bloques* para encriptar un texto. ¿Cuántos dígitos ha de tener cada bloque de entrada? ¿Cuántos dígitos ha de tener cada bloque de salida del texto encriptado?

   d)

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

En base a la tabla, encripte, usando *RSA* y *Cifrado en Bloques* el texto: CHIMBOLI.

Resolución:

a) Para buscar 41^{-1} mód(71) necesitamos hallar $1 \leq x \leq 70$ tal que $41x \equiv 1$ mód(71). Como $41 \equiv -30$ mód(71), debemos resolver $30x \equiv -1$ mód(71) $\Leftrightarrow 2 \times 3 \times 5 \times x \equiv -1$ mód(71) $\Leftrightarrow 3 \times 5 \times x \equiv -36$ mód(71) $\Leftrightarrow 3 \times 5 \times x \equiv 35$ mód(71) $\Leftrightarrow 5 \times x \equiv 24 \times 35$ mód(71) $\Leftrightarrow 5 \times x \equiv 59$ mód(71) $\Leftrightarrow x \equiv 57 \times 59$ mód(71), pues 36 es el inverso de 2, 24 es el inverso de 3 y 57 es el inverso de 5 en U(71). Como 57×59 mód(71) $\equiv 19 \times 3 \times 59$ mód(71) $\equiv 19 \times 35$ mód(71) $\equiv 19 \times 5 \times 7$ mód(71) $\equiv 24 \times 7$ mód(71) $\equiv 2 \times 12 \times 7$ mód(71) $\equiv 2 \times 13$ mód(71) $\equiv 26$ mód(71). Por lo tanto 26 es el inverso de 41 módulo 71. O sea existe $t \in \mathbb{Z}$, tal que $26 \times 41 - 1 = 71 \times t$. Como $26 \times 41 = 1066$, diviendo entre 71 se obtiene t: $26 \times 41 = 15 \times 71 + 1$, por lo tanto $26 \times 41 + (-15) \times 71 = 1$. Luego tenemos los coeficientes de Bezout y los inversos que buscamos: -15=26 es el inverso de 71 módulo 41 y 26 es el inverso de 41 módulo 71.

b) Para calcular 236^3 mód(2911) y 317^3 mód(2911), observemos que $2911 = 41 \times 71$. Por lo tanto comenzamos resolviendo 236^3 mód(41) y 236^3 mód(71).

Tenemos que 236^3 mód$(41) \equiv 31^3$ mód$(41) \equiv (-10)^3$ mód$(41) \equiv (-10) \times 18$ mód$(41) \equiv (-2) \times 5 \times 18$ mód$(41) \equiv (-2) \times 8$ mód$(41) \equiv 25$ mód(41).

Por su lado 236^3 mód$(71) \equiv 23^3$ mód$(71) \equiv (48)^2 \times 23$ mód$(71) \equiv 48 \times 2 \times 24 \times 23$ mód$(71) \equiv 25 \times 24 \times 23$ mód$(71) \equiv 25 \times 3 \times 8 \times 23$ mód$(71) \equiv 4 \times 8 \times 23$ mód$(71) \equiv 21 \times 8$ mód$(71) \equiv 13 \times 2$ mód$(71) \equiv 26$ mód(41).

Luego, con lo obtenido hasta ahora, y lo calculado en el item anterior, por el teorema chino del resto, podemos concluir que: $236^3 = 25 \times 71 \times 26 + 26 \times 41 \times 26$ mód(2911). O sea, $236^3 \equiv 73866$ mód$(2911) \equiv 1091$ mód(2911).

Con el mismo tipo de técnicas y apoyándonos nuevamente en el item anterior se puede calcular que $317^3 \equiv 2851$ mód(2911).

c)
- El par $(2911, 3)$ sirve como clave pública para RSA pues 2911$= 41 \times 71$ siendo 41 y 71 números primos, y además el $\mathrm{mcd}(3, \phi(2911)) = 1$, pues $\phi(2911) = 40 \times 70 = 2^4 \times 5^2 \times 7$ (donde ϕ es la función de Euler).
- Como son 28 dígitos, buscamos $k \in I\!N$ tal que $28^k < n < 28^{k+1}$. Entonces $k = 2$. Por lo tanto los bloques de entrada tendrán 2 dígitos y los de salida tendrán 3.

d) El texto encriptado es: DJIBK BEÑCUL.

Universidad de la República
Facultad de Ingeniería.

Examen de Matemática Discreta II
.... de diciembre de 2013

Número de Examen	Cédula	Nombre y Apellido

1. **(*aa* puntos)**
   a) Hallar todas las soluciones posibles con $a, b \in \mathbb{N}$ de
      - $a + b = 1235$
      - $\mathrm{mcm}(a, b) = 714\ \mathrm{mcd}(a, b)$.

   b) ¿Qué restos puede dejar un cubo perfecto al dividir entre $(d - 10)$? (siendo $d = \mathrm{mcd}(a, b)$ de la parte anterior).

   c) Mostrar que la ecuación $x^3 - 117y^3 = 5$ no tiene soluciones enteras.

2. **(*bb* puntos)**
   a) Sea $f : (G_1, *) \longrightarrow (G_2, \star)$ un morfismo de grupos. Definir $\mathrm{Ker}(f)$ y demostrar que $\mathrm{Ker}(f)$ es un subgrupo normal de G_1.

   b) Sea $R(x$ el grupo de las funciones racionales con el producto............

   c) Sea $f : (\mathbb{Z}, +) \longrightarrow (\mathbb{Z}, +)$ un morfismo de grupos,
      i. Demostrar que $h : \mathbb{Z} \longrightarrow R(x)$, tal que $h(n) = x^{f(n)}$ es un morfismo de grupos.
      ii. Hallar el $\mathrm{Ker}(h)$.

   d) Sabiendo que $h(-1) = \frac{1}{x^a}$ donde a es la menor raíz primitiva de $U(17)$, describir el morfismo f.

3. **(*cc* puntos)**
   a) Mostrar que 3 es raíz primitiva módulo 31.

   b) Calcular $\sum_{i=0}^{309} 3^i \ \mathrm{mód}(31)$

4. **(*dd* puntos)**
   a) Describir el Criptosistema RSA.

   b) Definir la función dde desencriptado y demostrar que desencripta.

Universidad de la República.
Facultad de Ingeniería.

Solución Examen de Matemática Discreta II

30 de julio de 2013

Ejercicio 1 **(28 puntos)** Sea $a \in \mathbb{N}$ tal que el resto de dividir a entre 12 es 5.

a) **(10 puntos)** Probar que $a^3 + 4 \equiv 21 \text{ mód}(36)$

b) **(8 puntos)** Hallar y el resto de dividir $53^3 + 11$ entre 36.

c) **(10 puntos)** Siendo y el hallado en la parte anterior, resolver:

$$\begin{cases} x \equiv -1 \text{ mód } (10) \\ x + 3 \equiv y \text{ mód } (8) \\ x \equiv 4 \text{ mód } (9) \end{cases}$$

Solución Ejercicio 1 (28 puntos)

a) **(10 puntos)** Como a es congruente con 5 módulo 12, entonces exite $t \in \mathbb{Z}$ tal que $12.t = a - 5$. Luego $(12t)^3 = (a-5)^3 = a^3 - 3a^2 5 + 3a5^2 - 5^3 = a^3 - 5^3 - 3a5(a-5)$. Esto implica que $a^3 - 5^3 = (12t)^3 + 3a5(a-5)$. Como $(a-5)$ es múltiplo de 12, el segundo término de la igualdad es múltiplo de 36. Esto implica que $a^3 - 5^3 \equiv 0 \text{ mód}(36)$, o sea $a^3 \equiv 125 \text{ mód}(36)$ por lo tanto $a^3 \equiv 17 \text{ mód}(36)$.

b) **(8 puntos)** Como 53 verifica la hipótesis del ejercicio, tenemos que $53^3 \equiv 17 \text{ mód } (36)$. Luego $53^3 + 11 \equiv 28 \text{ mód } (36)$, o sea que el resto de dividir $53^3 + 11$ entre 36, es 28.

c) **(10 puntos)**
El sistema queda:

$$\begin{cases} x \equiv -1 \text{ mód } (10) \\ x + 3 \equiv 28 \text{ mód } (8) \\ x \equiv 4 \text{ mód } (9) \end{cases}$$

Este sistema es equivalente a

$$\begin{cases} x \equiv -1 \text{ mód } (10) \\ x \equiv 1 \text{ mód } (8) \\ x \equiv 4 \text{ mód } (9) \end{cases}$$

y éste, a su vez, es equivalente a:

$$\begin{cases} x \equiv 1 \text{ mód } (2) \\ x \equiv -1 \text{ mód } (5) \\ x \equiv 1 \text{ mód } (8) \\ x \equiv 4 \text{ mód } (9) \end{cases}$$

Este último sistema es compatible y equivalente a:

$$\begin{cases} x \equiv 4 \text{ mód } (5) \\ x \equiv 1 \text{ mód } (8) \\ x \equiv 4 \text{ mód } (9) \end{cases}$$

Por el Teorema chino del resto, hay solución: 49, única módulo $5 \times 8 \times 9 = 360$.

Ejercicio 2 **(22 puntos)**

Sea $G := \{e, a, b, c, d\}$ y una operación binaria $\star : G \times G \to G$, tal que:

$$\begin{aligned} a \star b &= d \\ b \star c &= e \\ d \star a &= e \end{aligned}$$

a) **(6 puntos)** Hallar la tabla de Cayley de la operación, sabiendo que $(G, \star)$ es un grupo y e es su neutro.

b) **(4 puntos)** Demostrar que $(G, \star)$ es abeliano.

c) **(7 puntos)** Describir todos los morfismos de grupos $f : (G, \star) \longrightarrow (\mathbb{Z}_{12}, +)$.

d) **(5 puntos)** Demostrar que existe $n \in \mathbb{N}$ tal que $(G, \star)$ es isomorfo a $(\mathbb{Z}_n, +)$. Justificar.

Solución Ejercicio 2 (22 **puntos**)

a) **(6 puntos)** La tabla de Cayley es:

$\star$	**e**	**a**	**b**	**c**	**d**
e	e	a	b	c	d
a	a	c	d	b	e
b	b	d	a	e	c
c	c	b	e	d	a
d	d	e	c	a	b

b) **(4 puntos)** Basta observar que la tabla de Cayley es simétrica.

c) **(7 puntos)** Como $|G| = 5$ y $|\mathbb{Z}_{12}| = 12$, entonces la $\mathrm{Im}(f)$ solo puede tener un elemento (recordar que $|\mathrm{Im}(f)|$ divide a al orden del grupo dominio y al orden del grupo codominio, si todos son finitos).

d) **(5 puntos)** Como $|G| = 5$ el único n posible es $n = 5$. Ahora bien, definiendo $g : (G, \star) \longrightarrow (\mathbb{Z}_5, +)$, tal que $g(a) = 1$, $g(c) = 2$, $g(b) = 3$, $g(d) = 4$, $g(e) = 0$, se obtiene una función biyectiva, que se puede comprobar revisando las tablas de ambos grupos que es un morfismo.

Ejercicio 3 **(30 puntos)**

A	B	C	D	E	F	G	H	I	J	K	L	M	N	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

Dos interlocutores A y B acuerdan comunicarse estableciendo una clave privada mediante el método de Diffie-Hellman. Acuerdan usar el módulo primo $p = 97$ y como base $g = 5$. A elige además el entero $m = 3$, enviándole a B g^m y recibiendo de éste 36.

a) **(5 puntos)** ¿Cuál es la clave privada que acuerdan?

b) **(8 puntos)** Usando la correspondencia de la tabla inicial del ejercicio, la clave privada escrita en base 27 determina una palabra. ¿Cuál es esa palabra?

c) (*α* **puntos**) B envía a A el siguiente mensaje: `H CVDHROPTOCQ`, el cuál está encriptado mediante el método de Vigenère, usando la palabra hallada en b). Determinar el mensaje original encriptado por B.

d) (*β* **puntos**) A responderá a B: `LO CONOZCO`. Encriptar este mensaje mediante el mismo método usado por A.

(De tal manera que $\alpha + \beta = 17$ y ambos son menores o iguales a 12).

Solución Ejercicio 3 (30 puntos)

a) **(5 puntos)** En este caso, la forma de hallar la clave es resolver $36^3 \mod (97) = 96$.

b) **(8 puntos)** Como $96 = 3 \times 27^1 + 15 \times 27^0$, entonces la palabara es DP (ver en la tabla D=3, y P=15).

c) (*α* **puntos**) Empecemos observando que el opuesto de D es Y (el opuesto de 3 es 24), y el opuesto de P es M (el opuesto de 15 es 12) en $\mathbb{Z}_{27}$. Se arma la tabla de desencriptado Vigenère:

H		C	V	D	H	R	O	P	T	O	C	Q
7	26	2	21	3	7	17	14	15	19	17	2	16
24	12	24	12	24	12	24	12	24	12	24	12	24
4	11	26	6	0	19	14	26	12	4	11	14	13
E	L		G	A	T	O		M	E	L	Ó	N

d) (*β* **puntos**) Para encriptar hay que usar la palabra hallada en *b*): DP, que, usando la tabla inicial, es 3 15.

L	O		C	O	N	O	Z	C	O
11	14	26	2	14	13	14	25	2	14
3	15	3	15	3	15	3	15	3	15
14	2	2	17	17	1	17	13	5	2
O	C	C	R	R	B	R	N	F	C

Ejercicio 4 **(20 puntos)**

a) **(15 puntos)** Enunciar y demostrar el Teorema de Lagrange.
Ver Teórico.

b) **(5 puntos)** Obtener el Teorema de Fermat como corolario del Teorema de Lagrange.
Simplemente aplicar el Teorema de Lagrange para el grupo $(U(p), .)$ con p primo. Dado un elemento $a \in U(p)$, sabemos que $o(a) = |\langle a \rangle|$, o sea el orden de un elemento coinicide con el orden (cardinal) del grupo que elemento genera. Por el Teorema de Lagrange tenemos entones que $o(a) = |\langle a \rangle|$ divide a $|U(p)| = p - 1$. O sea $p - 1 = o(a).t$, con $t \in \mathbb{Z}^+$. Por lo tanto $a^{p-1} = (a^{o(a)})^t \equiv 1 \mod (p)$.

EXAMEN DE MATEMÁTICA DISCRETA 2

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

Duración: 3:30 hs. Sin material y sin calculadora.
Es necesario mostrar la resolución de los ejercicios, presentar únicamente la respuesta final carece de valor.

Ejercicio 1.

A. Enuncie (y no demuestre) la identidad de Bezòut.

B. Demuestre que si $a, b, c \in \mathbb{Z}$ con $\operatorname{mcd}(a, b) = 1$ y $a|bc$, entonces $a|c$.

C. Hallar todos los $a, b \in \mathbb{N}$ tales que $a > b$, $a|7b$ y $\operatorname{mcm}(a, b) = 245$.

D. En un campamento 23 acampantes van a cargar la leña para el asadito. Se encuentran 63 atados de leña con igual cantidad de leños cada uno. Además, encuentran sueltos 7 leños. Si cada acampante no puede cargar más de 50 leños cada uno, y logran repartirse los leños equitativamente, ¿cuántos leños había en cada atado?

Ejercicio 2.

A. Hallar todos los $x \in \mathbb{Z}$ tales que $\begin{cases} x \equiv 8 \pmod{31} \\ x \equiv 11 \pmod{17}. \end{cases}$

B. Sean p y q dos primos distintos y $n = pq$. Sea $e \in \mathbb{N}$ tal que $\operatorname{mcd}(e, \varphi(n)) = 1$ y $E : \mathbb{Z}_n \to \mathbb{Z}_n$ la función de encriptado utilizada en el sistema RSA con clave (n, e); es decir $E(x) = x^e \pmod{n}$.

Probar que si $ed \equiv 1 \pmod{\varphi(n)}$, entonces la función $D : \mathbb{Z}_n \to \mathbb{Z}_n$ dada por $D(y) = y^d \pmod{n}$ desencripta.

C. Sean $p = 17$, $q = 31$ y $n = pq$ y $e = 107$. Si la clave para RSA es (n, e),

(i) Hallar la función D de desencriptado.

(ii) Si E es la función de encriptado y $E(x) = 250$, hallar x (puede resultar útil saber que $255 = 15 \times 17$ y $248 = 8 \times 31$).

Ejercicio 3.

A. Enuncie (y no demuestre) el Teorema de Lagrange.

B. Deduzca que si G es un grupo finito con neutro e y $g \in G$, entonces $g^{|G|} = e$.

C. Pruebe que si $f : G_1 \to G_2$ es un homomorfismo de grupos finitos, y $g \in G_1$, entonces $o(f(g))| \operatorname{mcd}(|G_1|, |G_2|)$ (todas las propiedades que se utilicen sobre homomorfismos, deben ser probadas).

D. Hallar todos los homorfismos $f : \mathbb{Z}_2 \to U(8)$.

E. Hallar p sabiendo que p es primo, y existe un homomorfismo no trivial $f : \mathbb{Z}_{51} \to \mathbb{Z}_p$ tal que $f\left(\overline{17}\right) = \overline{0}$.

SOLUCIÓN EXAMEN DE MATEMÁTICA DISCRETA 2

Ejercicio 1.

A. Sean a, $b \in \mathbb{Z}$ y $d = \text{mcd}(a, b)$ entonces existen $x, y \in \mathbb{Z}$ tales que $ax + by = d$.

B. Por identidad de Bezòut tenemos que existen $x, y \in \mathbb{Z}$ tales que $ax + by = 1$, luego $cax + cby = c$. Como $a|cax$ y $a|bcy$ entonces $a|cax + cby$, es decir $a|c$

C. Sea $d = \text{mcd}(a, b)$ y escribimos $a = a'd$, $b = b'd$ sabiendo que $\text{mcd}(a', b') = 1$. Como $a|7b$ entonces $a'|7b'$, por parte **B.** tenemos que $a'|7$. Como $a' > b'$, $a' \neq 1$ y entonces $a' = 7$. Por otro lado tenemos que $\text{mcm}(a, b) = a'b'd = 245 = 7^2 \cdot 5$. Por la descomposición anterior puede pasar que $b' = 5$ y $d = 7$ o $b' = 1$ y $d = 35$. Los números buscados son $(a, b) = (49, 35)$ y $(a, b) = (245, 35)$.

D. Si denotamos por x a la cantidad de leños por atado y por y a la cantidad de leños que lleva cada uno, debemos resolver la siguiente ecuación

$$63x + 7 = 23y.$$

Para esto resolvemos $-63x + 23y = 1$, observemos que tenemos

$$63 = 23 \cdot 2 + 17 \quad 23 = 17 + 6 \quad 17 = 6 \cdot 2 + 5 \quad 6 = 5 + 1$$

Luego

$$\begin{pmatrix} 5 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix}\begin{pmatrix} 63 \\ 23 \end{pmatrix} = \begin{pmatrix} 3 & -8 \\ -4 & 11 \end{pmatrix}\begin{pmatrix} 63 \\ 23 \end{pmatrix}$$

Luego $1 = (-63) \cdot 4 + 23 \cdot 11$ y $7 = (-63) \cdot 28 + 23 \cdot 77$, luego todas las soluciones son $x = 28 + 23k$ e $y = 63k + 77$. Como $0 \leq y \leq 50$ entonces $k = -1$ y la respuesta es que había $x = 28 - 23 = 5$ leños en cada atado.

Ejercicio 2.

A. $x \equiv 8 \pmod{31} \Leftrightarrow \exists k \in \mathbb{Z} : \ x = 8 + 31k$. Si además, $x \equiv 11 \pmod{17} \Rightarrow \exists k' \in \mathbb{Z} :$ $8 + 31k = 11 + 17k'$. Entonces, $31k - 17k' = 3$. Haciendo el algoritmo de Euclides extendido vemos que $31(-6) + 17(11) = 1$, así que $31(-18) + 17(33) = 3$ y $31(-18 + 17z) - 17(-33 + 31z) = 3$ para todo $z \in \mathbb{Z}$. Por lo tanto todas las soluciones de $31k - 17k' = 3$ son de la forma : $k = -18 + 17z$ y $k' = -33 + 31z$ con $z \in \mathbb{Z}$ y entonces las soluciones del sistema original son $x = 8 + 31k = 8 + 31(-18 + 17z) : z \in \mathbb{Z}$, por lo tanto $x \equiv 504 \pmod{527}$.

B. Escribimos $de = 1 + k\varphi(n) = 1 + k(p-1)(q-1)$. Hay que probar que $D(E(x)) = x$ para todo $x \in \mathbb{Z}_n$. Es decir, hay que probar que para todo $a \in Z$, $(a^e)^d \equiv a \pmod{n}$. Si $\text{mcd}(a, n) = 1$, por el teorema de Eüler sabemos que $a^{\varphi(n)} \equiv 1 \pmod{n} \Rightarrow \left(a^{\varphi(n)}\right)^k \equiv 1 \pmod{n} \Rightarrow$ $\left(a^{\varphi(n)}\right)^k a \equiv a \pmod{n} \Rightarrow a^{\varphi(n)k+1} \equiv a \pmod{n} \Rightarrow a^{ed} \equiv a \pmod{n}$. Si $\text{mcd}(a, n) \neq 1$, como $n = pq$ con p y q primos, alguno de los dos factores divide a a. Si ambos factores dividen a a, entonces n divide a a entonces $a \equiv 0 \pmod{n}$ y claramente $a^{de} = a \pmod{n}$. Si sólo uno de los factores, supongamos p, divide a a, entonces $a \equiv 0 \pmod{p}$ y por lo tanto $a^{de} \equiv a \pmod{p}$. Ahora bien, si q no divide a a, usando Fermat tenemos que $a^{q-1} \equiv 1$ $\pmod{q} \Rightarrow (a^{q-1})^{(p-1)k} \equiv 1 \pmod{q} \Rightarrow (a^{q-1})^{(p-1)k} a \equiv a \pmod{q} \Rightarrow (a^{q-1})^{(p-1)k} a \equiv a$ $\pmod{q} \Rightarrow a^{de} = a \pmod{q}$. Entonces tenemos que $\begin{cases} a^{de} \equiv a \pmod{p} \\ a^{de} \equiv a \pmod{q} \end{cases}$ y como p y q son coprimos, concluímos que $a^{de} \equiv a \pmod{pq}$.

C. (i) Tenemos que hallar d talque $de \equiv 1 \pmod{\varphi)(n)}$; es decir, tenemos que resolver $107d \equiv 1 \pmod{16 \times 30}$, o sea, $107d \equiv 1 \pmod{480}$. Con el Algoritmo de Euclides extendido vemos que $480(35)+107(-157) = 1$, y por lo tanto $d \equiv -157 \pmod{4)80} \equiv 323 \pmod{480}$.

(ii) Tenemos que $x \equiv 250^{323} \pmod{31 \times 17}$, y como 31 y 17 son coprimos, tenemos que esto pasa si y sólo si, $\begin{cases} x \equiv 250^{323} \pmod{31} \\ x \equiv 250^{323} \pmod{17}. \end{cases}$ Como $255 = 15 \times 17$ tenemos que $250 \equiv -5 \pmod{17}$ y como $248 = 8 \times 31$, $250 = 2 \pmod{31}$. Así que la primer ecuación nos queda: $x \equiv 250^{323} \pmod{31} \Rightarrow 2^{323} \pmod{31} \Rightarrow$ (como $(2^5 \pmod{1} \pmod{3)1)}) \Rightarrow x \equiv 8 \pmod{31}$. La segunda ecuación nos queda: $x \equiv 250^{323} \pmod{17} \Rightarrow x \equiv (-5)^{323} \pmod{17} \Rightarrow$ (por Fermat tenemos que $(-5)^{16} \equiv 1 \pmod{17}$) $\Rightarrow x \equiv (-5)^3 \pmod{17} \equiv 25(-5) \pmod{17} \equiv 8(-5) \pmod{17} \equiv -40 \pmod{17} \equiv 11 \pmod{17}$. Así que $\begin{cases} x \equiv 8 \pmod{31} \\ x \equiv 11 \pmod{17} \end{cases}$ y por la parte A. tenemos que $x \equiv 504 \pmod{527}$.

Ejercicio 3.

A. Si G es un grupo finito y H es un subgrupo de G, entonces $|H|$ divide a $|G|$.

B. Si $H =< g >$, el subrupo de G generado por g, tenemos que $|H| = o(g)$. Por el Teorema de Lagrange $|H|$ divide a $|G|$ y luego $o(g)||G|$. Por lo tanto $|G| = o(g)k$ con $k \in \mathbb{Z}$ y

$$g^{|G|} = g^{o(g)k} = (g^{o(g)})^k = e^k = e.$$

C. Por Teorema de Lagrange sabemos que $o(f(g))$ divide a $|G_2|$. Por definición de homomorfismo $f(e_1) = f(e_1 \cdot e_1) = f(e_1) \cdot f(e_1)$ entonces $f(e_1) = e_2$. Como $f(g)^{o(g)} = f(g^{o(g)}) = f(e_1) = e_2$ tenemos que $o(f(g))$ divide a $o(g)$ que divide a $|G_1|$. Por lo tanto $o(f(g))$ divide a $\operatorname{mcd}(|G_1|, |G_2|)$.

D. Si f es un homomorfismo, entonces $f(\bar{0}) = \bar{1}$. Si $f(\bar{1}) = \bar{1}$ entonces f es trivial y es homomorfismo. Si f no es trivial, entonces $f(\bar{1}) \in \{\bar{3}, \bar{5}, \bar{7}\} \subset U(8)$. Así que en cualquiera de estos casos, $f(\bar{1}) \neq \bar{1}$ y $f(\bar{1})^2 = \bar{1}$ (es decir, $f(\bar{1})$ es un elemento de orden 2). Con cualquier elección de $f(\bar{1}) \in \{\bar{3}, \bar{5}, \bar{7}\}$, la función obtenida es homomorfismo; veamos esto:

$$f(\bar{0} + \bar{1}) = f(\bar{1}) = \bar{1}f(\bar{1}) = f(\bar{0})f(\bar{1}), \quad \text{y}$$

y

$$f(\bar{1} + \bar{1}) = f(\bar{(0)}) = \bar{1} = (f(\bar{1}))^2 = f(\bar{1})f(\bar{1}).$$

Así que todos los homomorfismos son f_1, f_2, f_3, f_4 donde

$$f_i(\bar{0}) = \bar{1}, \quad \forall i \in \{1, 2, 3, 4\} \quad \text{y} \quad f_1(\bar{1}) = \bar{1}, \quad f_2(\bar{1}) = \bar{3}, \quad f_3(\bar{1}) = \bar{5}, \quad f_4(\bar{1}) = \bar{7}.$$

E. Al ser $\operatorname{im}(f)$ un subgrupo de $\mathbb{Z}_p$ tenemos que $|\operatorname{im}(f)|$ divide a $|\mathbb{Z}_p| = p$. Al ser p primo $|\operatorname{im}(f)|$ es 1 o p. Pero como f es no trivial entonces $|\operatorname{im}(f)| \neq 1$ y por lo tanto $|\operatorname{im}(f)| = p$. Por otro lado (por el teo de órdenes para homomorfismos) tenemos que $51 = |\mathbb{Z}_{51}| = |\ker(f)||\operatorname{im}(f)| = |\ker(f)| \cdot p$. De aquí (como p es primo, $p \neq 1$) vemos que o $p = 3$ y $|\ker(f)| = 17$ o $p = 17$ y $|\ker(f)| = 3$. De $f(\overline{17}) = 0$, tenemos que $\overline{17} \in \ker(f)$ y como $o(\bar{1}7) = 3$ entonces (por Lagrange) que 3 divide a $|\ker(f)|$. Así que $|\ker(f)| = 3$ y $p = 17$.