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

Primer parcial (segunda prueba)
24 de setiembre de 2018.
Duración: 3 horas

Nombre y Apellido	Cédula de identidad

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

Ejercicio 1. (9 puntos)
El número de la cédula uruguaya tiene la forma $x_1x_2\dots x_7 - x_8$ donde cada $x_i, i = 1, 2\dots 8$ es un dígito de 0 a 9. El dígito verificador x_8 se calcula de la siguiente manera. Sea

$$c = \sum_{i=1}^{7} a_i \cdot x_i,$$

donde $(a_1, a_2, a_3, a_4, a_5, a_6, a_7) = (2, 9, 8, 7, 6, 3, 4)$. Entonces x_8 es: $r \equiv -c \pmod{10},\ 0 \le r < 10$.

a. Verificar cuál o cuáles de las siguientes cédulas son falsas:

- Cédula (A): 5806386-7
- Cédula (B): 418160-6

b. Investigar si el dígito verificador detecta el error de copiar mal el segundo dígito.

c. Probar que el dígito verificador detecta el error de intercambiar los dos primeros dígitos x_1, x_2.

Ejercicio 2. (9 puntos)

a. Demostrar el Teorema de Euler.
Sean $a, n \in \mathbb{Z}$ tales que $\operatorname{mcd}(a, n) = 1$, entonces: $a^{\varphi(n)} \equiv 1 (\text{mód } n)$.

b. Calcular $22^{232} \equiv (\text{mód } 9)$.

c. Calcular $22^{232} \equiv (\text{mód } 36)$.

Ejercicio 3. (12 puntos)

a. Hallar el $\operatorname{mcd}(7^4 - 1, 11^4 - 1)$.

b. Demostrar que si $p \ge 7$ es primo entonces $240|(p^4 - 1)$.

c. Sea $A \subset \mathbb{Z}^*$ un subjconjunto no vacío de números enteros diferentes de cero. Definimos $\operatorname{mcd}(A) = \text{máx}\{d \in \mathbb{Z}^+ \ / \ d|a, \text{ para todo } a \in A\}$.
Probar, a partir de las partes anteriores, que: $\operatorname{mcd}\{p^4 - 1 \ / \ p \ge 7,\ p \text{ primo } \} = 240$.

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

PRIMER PARCIAL (SEGUNDA PRUEBA)
24 DE SETIEMBRE DE 2018.
DURACIÓN: 3 HORAS

Ejercicio 1. (9 puntos)
El número de la cédula uruguaya tiene la forma $x_1x_2\dots x_7 - x_8$ donde cada $x_i, i = 1, 2\dots 8$ es un dígito de 0 a 9. El dígito verificador x_8 se calcula de la siguiente manera. Sea

$$c = \sum_{i=1}^{7} a_i \cdot x_i,$$

donde $(a_1, a_2, a_3, a_4, a_5, a_6, a_7) = (2, 9, 8, 7, 6, 3, 4)$. Entonces x_8 es: $r \equiv -c \pmod{10},\ 0 \leq r < 10$.

a. Verificar cuál o cuáles de las siguientes cédulas son falsas:

- Cédula (A): 5806386-7. *FALSA*
- Cédula (B): 418160-6. *CORRECTA*

b. Investigar si el dígito verificador detecta el error de copiar mal el segundo dígito.

Solución:
Asumamos que calculamos el código con $x_1, y_2, x_3, x_4, x_5, x_6, x_7$ con $y_2 \neq x_2$, y probemos que el dígito verificador que surge es diferente de x_8.

Calculamos $\sum_{i=1}^{7} a_i \cdot x_i$ y comparamos con $a_1 \cdot x_1 + a_2 \cdot y_2 + \sum_{i=3}^{7} a_i \cdot x_i$, donde $(a_1, a_2, ..., a_7) = (2, 9, 8, 7, 6, 3, 4)$, como arriba.
Asumamos por absurdo que los códigos verificadores coinciden:

$$\sum_{i=1}^{7} a_i \cdot x_i \equiv a_1 \cdot x_1 + a_2 \cdot y_2 + \sum_{i=3}^{7} a_i \cdot x_i \pmod{10},$$

entonces, $a_2 \cdot x_2 \equiv a_2 \cdot y_2 \pmod{10}$. Como $a_2 = 9$ tenemos que $9x_2 \equiv 9y_2 \pmod{10}$, y como 9 es invertible módulo 10, de hecho $9 \cdot 9 \equiv 1 \pmod{10}$, se obtiene que $x_2 \equiv y_2 \pmod{10}$. O sea x_2 es el mismo dígito que y_2, contradiciendo la hipótesis. Por lo tanto lo asumido es falso, con lo cual los dígitos verificadores que surgen son diferentes.

c. Probar que el dígito verificador detecta el error de intercambiar los dos primeros dígitos x_1, x_2.

Solución:

Asumamos que $x_2 \neq x_1$ (sin falta de generalidad podemos asumir que $x_2 > x_1$), pues si son iguales no surge ningún problema en intercambiar los dígitos.
Supongamos que:

$$\sum_{i=1}^{7} a_i \cdot x_i \equiv a_1 \cdot x_2 + a_2 \cdot x_1 + \sum_{i=3}^{7} a_i \cdot x_i \pmod{10}$$

Eso implica que:

$$a_1 \cdot x_2 + a_2 \cdot x_1 \equiv a_1 \cdot x_1 + a_2 \cdot x_2 \pmod{10}.$$

Luego:

$$x_1 \cdot (a_2 - a_1) \equiv x_2 \cdot (a_2 - a_1) \pmod{10}.$$

Como $a_2 = 9$ y $a_1 = 2$ tenemos que $a_2 - a_1 = 7$. Luego, como $\text{mcd}(7, 10) = 1$, se tiene que 7 es invertible módulo 10. De hecho $7 \cdot 3 \equiv 1 \pmod{10}$.

Habíamos obtenido que: $7 \cdot x_1 \equiv 7 \cdot x_2 \pmod{10}$, con lo cual, multiplicando por 3 obtenemos que: $x_1 \equiv x_2 \pmod{10}$. Como x_1 y x_2 son dígitos (entre 0 y 9) congruentes módulo 10, entonces $x_1 = x_2$, absurdo.
Por lo tanto:

$$\sum_{i=1}^{7} a_i \cdot x_i \not\equiv a_1 \cdot x_2 + a_2 \cdot x_1 + \sum_{i=3}^{7} a_i \cdot x_i \pmod{10}$$

Ésto es lo que se quería demostrar.

Ejercicio 2. (9 puntos)

a. Demostrar el Teorema de Euler.
Sean $a, n \in \mathbb{Z}$ tales que $\text{mcd}(a, n) = 1$, entonces: $a^{\varphi(n)} \equiv 1 (\text{mód } n)$.

Solución:

Ver la demostración en las notas de teórico (Teorema 2.6.5, página 41).

b. Calcular $22^{232} \equiv x \pmod{9}$.

Solución:

Vamos a utilizar el Teorema de Euler con $n = 9$ y $a = 22$ (obsérvese que $\text{mcd}(a, n) = 1$, como pide la hipótesis del teorema citado). Como $\varphi(9) = 6$, tenemos que $22^{\varphi(9)} \equiv 1 \pmod{9}$, o sea $22^6 \equiv 1 \pmod{9}$. Luego $22^{232} = 22^{6 \cdot 38 + 4} = (22^6)^{38} \cdot 22^4 \equiv 22^4 \pmod{9}$. Por otro lado $22 \equiv 4 \pmod{9}$, lo que implica que $22^4 (\text{mód } 9) \equiv 4^4 \pmod{9}$. Como $4^2 = 16 \equiv 7 \pmod{9}$ concluimos que $22^{232} \equiv 7^2 \pmod{9} \equiv 4 \pmod{9}$.

c. Calcular $22^{232} \equiv y \pmod{36}$.

Solución:

Vimos que $22^{232} \equiv 4 \pmod{9}$. Por otro lado $22^{232} \equiv 0 \pmod{4} \equiv 4 \pmod{4}$. O sea que $22^{232} - 4$ es múltiplo de 9 y es múltiplo de 4. Pero 4 y 9 son primos entre sí, por lo que $22^{232} - 4$ es múltiplo de 36. O sea, $22^{232} \equiv 4 \pmod{36}$.

Ejercicio 3. (12 puntos)

a. Hallar el mcd $(7^4 - 1, 11^4 - 1)$.

Solución:

Tenemos que $7^4 - 1 = 49 \cdot 49 - 1 = (50 - 1) \cdot (50 - 1) - 1 = 2500 - 100 + 1 - 1 = 2400$.

A su vez $11^4 - 1 = 121 \cdot 121 - 1 = 14641 - 1 = 14640$.

Como $14640 = 2400 \cdot 6 + 240$, tenemos que $\text{mcd}(14640, 2400) = \text{mcd}(2400, 240) = 240$.

b. Demostrar que si $p \geq 7$ es primo entonces $240 | (p^4 - 1)$.

Solución:

Obsérvese que $240 = 24 \cdot 10 = 3 \cdot 8 \cdot 2 \cdot 5$, o sea, $240 = 16 \cdot 3 \cdot 5 = 2^4 \cdot 3 \cdot 5$.
Debemos probar que 2^4 divide a $p^4 - 1$, que 3 divide a $p^4 - 1$ y que 5 divide a $p^4 - 1$, para todo primo $p \geq 7$. Eso es necesario pero también suficiente para probar que 240 divide a $p^4 - 1$ para todo primo $p \geq 7$, pues 2^4, 3 y 5 son primos entre sí.

Probemos primero que 3 divide a $p^4 - 1$: como todos los primos, excepto el 3, son de la forma $3k + 1$ o $3k + 2$, tenemos que $p \equiv 1 \pmod{3}$ o $p \equiv 2 \pmod{3}$, para todo primo $p \geq 7$. Luego

$p^2 \equiv 1 \pmod 3$, para todo primo $p \geq 7$. Por lo tanto $p^4 \equiv 1 \pmod 3$, para todo primo $p \geq 7$. O sea que 3 divide a $p^4 - 1$, para todo primo $p \geq 7$.

Probemos ahora que 5 divide a $p^4 - 1$ para todo primo $p \geq 7$, o equivalentemente, probemos que $p^4 \equiv 1 \pmod 5$, para todo primo $p \geq 7$. Sabemos que por ser $p \geq 7$ primo, tenemos que $p \equiv 1 \pmod 5$, o $p \equiv 2 \pmod 5$, o $p \equiv 3 \pmod 5 \equiv -2 \pmod 5$, o $p \equiv 4 \pmod 5 \equiv -1 \pmod 5$.

En el primer y cuarto caso tenemos que $p^2 \equiv 1 \pmod 5$, y en el segundo y tercer caso tenemos que $p^2 \equiv 4 \pmod 5 \equiv -1 \pmod 5$. Luego, elevando nuevamente al cuadrado tenemos que en todos los casos $p^4 \equiv 1 \pmod 5$, para todo primo $p \geq 7$, lo que queríamos probar.

Por último queremos probar que $p^4 \equiv 1 \pmod{16}$, para todo primo $p \geq 7$. Todos los primos, excepto el 2, son de la forma $16k+1$, o $16k+3$, o $16k+5$, o $16k+7$, o $16k+9$, o $16k+11$, o $16k+13$, o $16k+15$. Analizando los 8 casos, como en las discusiones anteriores, vemos que $p^4 \equiv 1 \pmod{16}$, para todo primo $p \geq 7$.

Luego 2^4, 3 y 5 dividen a $p^4 - 1$ para todo primo $p \geq 7$, lqqd.

c. Sea $A \subset \mathbb{Z}^*$ un subjconjunto no vacío de números enteros diferentes de cero. Definimos $\operatorname{mcd}(A) = \max\{d \in \mathbb{Z}^+ \ / \ d|a, \text{ para todo } a \in A\}$.
Probar, a partir de las partes anteriores, que: $\operatorname{mcd}\{p^4 - 1 \ / \ p \geq 7, \ p \text{ primo}\} = 240$.

Solución:

Hemos probado que 240 divide a $p^4 - 1$ para todo primo $p \geq 7$, luego $240 = \operatorname{mcd}\{p^4 - 1 \ / \ p \geq 7, \ p \text{ primo}\}$, pues no puede haber un divisor común a todos los números de la forma $p^4 - 1$, con p primo, mayor que 240, porque en la primer parte vimos que el mcd $(7^4 - 1, 11^4 - 1) = 240$.

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

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

N° de parcial	Cédula	Apellido y nombre

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

Ejercicio 1.

a. Resolver el sistema

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

b. Probar que si $\text{mcd}(a, n) = 1$ entonces a es invertible módulo n.

c. Hallar el inverso de 7 módulo 11.

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

e. Hallar $x \in \{0, 1, \cdots, 15\}$ tal que $x \equiv 3^{139} \pmod{16}$.

f. Hallar todos los $x \in \mathbb{Z}$ tal que $x \equiv 51^{139} \pmod{176}$.

Ejercicio 2.

a. Sean $0 \neq a, b \in \mathbb{Z}$, probar que $\text{mcd}(a, b) = \text{mín}\{c > 0 : c = ax + by \text{ con } x, y \in \mathbb{Z}\}$.

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

i) Probar que si p es un primo divisor común de $(a + 2b)$ y ab, entonces $p = 2$.

ii) Hallar $\text{mcd}(a + 2b, ab)$ discutiendo según la paridad de a.

Ejercicio 3.

a. Hallar todos $a, b \in \mathbb{N}$ tales que $\text{mcd}(a, b) = 12$, a tiene 15 divisores positivos y b tiene 12.

b. Sea (p_n) la sucesión de los números primos, $p_1 = 2$, $p_2 = 3$, etc. Probar que para todo $n > 1$ y todo $k = 1, \cdots, n-1$, se tiene que

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

Solución del Primer parcial. Matemática Discreta 2, semipresencial
25 de setiembre de 2017.

Ejercicio 1.

a.
$$\begin{cases} x \equiv 8 \pmod{11} \Leftrightarrow \exists n \in \mathbb{Z} : x = 8 + 11n \ (*) \\ x \equiv 11 \pmod{16} \Leftrightarrow \exists m \in \mathbb{Z} \ : x = 11 + 16m \end{cases}.$$

Por lo tanto deben existir $m, n \in \mathbb{Z}$ tales que $8 + 11n = 11 + 16m$; es decir, tales que $11n - 16m = 3$ (**). Por el algoritmo de Euclides extendido tenemos que $1 = \operatorname{mcd}(16, 11) = 11(3) - 16(2)$; asi que (multiplicando por 3) tenemos que $3 = 11(9) - 16(6)$. Por lo tanto todas las soluciones de la diofántica (**) son $n = 9 + 16k$, $m = 6 + 11k$ con $k \in \mathbb{Z}$. Sustituyendo n en (*) obtenemos que todas las soluciones del sistema son $x = 8 + 11(9 + 16k) = 107 + 176k$, con $k \in \mathbb{Z}$; es decir $\boxed{x \equiv 107 \pmod{176}}$.

b. a es invertible módulo n si y sólo si existe $x \in \mathbb{Z}$ tal que $ax \equiv 1 \pmod{n}$; si y sólo si, existen $x, y \in \mathbb{Z}$ tales que $ax = 1 + ny$; es decir, tales que $ax - ny = 1$ (*). Al ser $\operatorname{mcd}(a, n) = 1$ la ecuación diofántica (*) tiene solución (por el teo. de ecs. diofánticas), y por lo tanto a es invertible módulo n.

c. Por lo hecho en la parte anterior, un entero x es el inverso de 7 módulo 11, si y sólo si, $\exists y \in \mathbb{Z}$ tal que $7x - 11y = 1$. Con el Algoritmo de Euclides extendido tenemos que $7(-3)+11(2) = 1$ y por lo tanto $\boxed{x \equiv -3 \pmod{11} \equiv 8 \pmod{11}}$ es el inverso de 7 módulo 11.

d. Como 11 es primo y no divide a 7, por el Teorema de Fermat tenemos que $7^{10} \equiv 1 \pmod{11}$ y por lo tanto (elevando ambos lados a la 14) $7^{140} \equiv 1 \pmod{11}$. Entonces tenemos que x cumple que $7x \equiv (7)7^{139} \pmod{11} \equiv 7^{140} \equiv 1 \pmod{11}$; es decir que x cumple que $7x \equiv 1 \pmod{11}$, y por la parte anterior tenemos que $x \equiv 8 \pmod{11}$, por lo tanto $\boxed{x = 8}$.

e. Observamos que $3^4 = 81 = 1 + 16(5) \equiv 1 \pmod{16}$. Por lo tanto $3^{139} = 3^{4(34)+3} = (3^4)^{34}3^3 \equiv (1)^{34}3^3 \pmod{16} \equiv 27 \pmod{16} \equiv 11 \pmod{16}$. Por lo tanto $\boxed{x = 11}$.

f. Como $176 = 11(16)$ y $\operatorname{mcd}(11, 16) = 1$, tenemos que $x \equiv 51^{139} \pmod{176}$ si y sólo si

$$\begin{cases} x \equiv 51^{139} \pmod{11} \quad \text{y} \\ x \equiv 51^{139} \pmod{16}. \end{cases}$$

Como $51 \equiv 7 \pmod{11}$ y $51 \equiv 3 \pmod{16}$, el sistema nos queda

$\begin{cases} x \equiv 7^{139} \pmod{11} \\ x \equiv 3^{139} \pmod{16} \end{cases}$ y por las partes c) y d) nos queda $\begin{cases} x \equiv 8 \pmod{11} \\ x \equiv 11 \pmod{16} \end{cases}$, que es el sistema de la parte a). Por lo tanto $\boxed{x \equiv 107 \pmod{176}}$.

Ejercicio 2.

a. Esto es el Teorema de Bezout; la demostración se encuentra en los apuntes de teórico (Teorema 1.2.8, página 10).

b.

i) Si p es un primo divisor común de $(a+2b)$ y ab, en particular $p \mid ab$ y por la propiedad de los primos (Corolario 1.2.11 de los apuntes de teórico) tenemos que $p \mid a$ o $p \mid b$.

- Si $p \mid a$, como $p \mid a + 2b$ tenemos que $p \mid a + 2b - a = 2b$ y nuevamente utilizando la propiedad de los primos, como $p \nmid b$ (pues b es coprimo con a), concluímos que $p \mid 2$ y por lo tanto $p = 2$.
- Si $p \mid b$, entonces $p \mid 2b$ y como $p \mid a + 2b$ tenemos que $p \mid a + 2b - 2b = a$ lo cual es absurdo pues $\operatorname{mcd}(a, b) = 1$.

Por lo tanto $\boxed{p = 2}$.

ii) De la parte anterior tenemos que $\operatorname{mcd}(a + 2b, ab) = 2^k$ con $k \in \mathbb{N}$.

- Si a es impar, entonces $a + 2b$ es impar y por lo tanto $2 \nmid a + 2b$ y entonces $\operatorname{mcd}(a + 2b, ab) = 2^0 = 1$.

- Si a es par, $a = 2a'$ con $a' \in \mathbb{Z}$ y entonces $2^k = \text{mcd}(a+2b, ab) = \text{mcd}(2a' + 2b, 2a'b) = \text{mcd}(2(a'+b), 2a'b) = 2\,\text{mcd}(a'+b, a'b)$. Por lo tanto $k \geq 1$. Veamos que $k = 1$. Para ésto basta con probar que $2 \nmid \text{mcd}(a'+b, a'b)$; es decir, que $a'+b$ o $a'b$ es impar. Como a es par y b es coprimo con a, tenemos que b es impar. Y entonces, si a' es par, $a'+b$ es impar y si a' es impar, tenemos que $a'b$ es impar.

Ejercicio 3.

a. Escribimos las descomposiciones factoriales de a y b como

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

con $a_p, b_p \in \mathbb{N}$ y sólo una cantidad finita de ellos no nulos. Entonces

$$2^2 \times 3 = 12 = \text{mcd}(a,b) = \prod_{p \text{ primo}} p^{\min(a_p, b_p)},$$

y por la unicidad de la descomposición factorial, tenemos que

- $\min(a_2, b_2) = 2$; por lo tanto $a_2 = 2 + x$ y $b_2 = 2 + y$ con $x, y \in \mathbb{N}$ y $x = 0$ o $y = 0$.
- $\min(a_3, b_3) = 1$; por lo tanto $a_3 = 1 + w$ y $b_3 = 1 + z$ con $w, z \in \mathbb{N}$ y $w = 0$ o $z = 0$.
- $\forall p > 3$, $\min(a_p, b_p) = 0$ y por lo tanto $a_p = 0$ o $b_p = 0$.

Por otro lado,

$$15 = \#\text{Div}_+(a) = \prod_{p \text{ primo}} (a_p + 1) = (2 + x + 1)(1 + w + 1) \prod_{\substack{p \text{ primo} \\ p>3}} (a_p + 1).$$

Y análogamente para b tenemos que

$$12 = (2 + y + 1)(1 + z + 1) \prod_{\substack{p \text{ primo} \\ p>3}} (b_p + 1).$$

Por la unicidad de la descomposiciòn factorial, como $15 = 3 \times 5$ tenemos únicamente las siguientes posibilidades:

1) $2 + x + 1 = 3,\ 1 + w + 1 = 5$ y $a_p = 0\,\forall p > 3$ o
2) $2 + x + 1 = 5,\ 1 + w + 1 = 3$ y $a_p = 0\,\forall p > 3$.

1) Si $2 + x + 1 = 3,\ 1 + w + 1 = 5$ y $a_p = 0\,\forall p > 3 \Rightarrow x = 0,\ w = 3\,(\Rightarrow z = 0)$ y $a_p = 0\,\forall p > 3$. Entonces $\boxed{a = 2^2 3^4 = 324}$ y como $z = 0$, tenemos que

$$12 = (2 + y + 1)(1 + 1) \prod_{\substack{p \text{ primo} \\ p>3}} (b_p + 1) \quad \Rightarrow \quad 6 = (2 + y + 1) \prod_{\substack{p \text{ primo} \\ p>3}} (b_p + 1).$$

Entonces hay dos posibilidades: $y = 3$ y $b_p = 0\ \forall p > 3$ o $y = 0$ y $b_p = 1$ para algún primo $p > 3$ y cero para el resto. Entonces $\boxed{b = 2^5 3 = 96}$ o $\boxed{b = 2^2 3p = 12p}$ con $p > 3$ primo.

2) Si $2 + x + 1 = 5,\ 1 + w + 1 = 3$ y $a_p = 0\ \forall p > 3 \Rightarrow x = 2\,(\Rightarrow y = 0),\ w = 1\,(\Rightarrow z = 0)$ y $a_p = 0\ \forall p > 3$. En este caso $\boxed{a = 2^4 3^2 = 144}$ y

$$12 = (2 + 1)(1 + 1) \prod_{\substack{p \text{ primo} \\ p>3}} (b_p + 1)$$

por lo que $b_p = 1$ para algun primo $p > 3$ y cero para el resto, por lo tanto $\boxed{b = 2^2 3p = 12p}$ con $p > 3$ primo.

Resumiendo, todos los pares (a,b) posibles son

$$\boxed{(324,96) \quad (324,12p) \quad (144,12p) \quad \text{con } p>3 \text{ primo.}}$$

b. Llamamos $a = p_1p_2\cdots p_k$, $b = p_{k+1}p_{k+2}\cdots p_n$ y $c = p_1p_2\cdots p_k + p_{k+1}p_{k+2}\cdots p_n = a+b$. Como $c \in \mathbb{Z}^+$, por el Teorema Fundamental de la Aritmética, c es producto de primos y por lo tanto, existe un primo $p = p_i$ tal que $p \mid c$. Veamos que $i \geq n+1$:

Si $1 \leq i \leq k$ entonces $p_i \mid p_1p_2\cdots p_k = a$ y por lo tanto $p_i \mid (c-a) = b$ lo cual es absurdo por la unicidad de la descomposición factorial de b. De forma similar, si $k+1 < i \leq n$ entonces $p_i \mid p_{k+1}p_{k+2}\cdots p_n = b$ y por lo tanto $p_i \mid (c-b) = a$ lo cual es absurdo por la unicidad de la descomposición factorial de a.

Entonces $i \geq n+1$, por lo tanto $p = p_i \geq p_{n+1}$. Ahora, como $p \mid c$, $c \geq p$ y por lo tanto $\boxed{c \geq p \geq p_{n+1}}$.

Solución primer parcial - 27 de abril de 2017.

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

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

entonces $d \mid 407$ y $d \in \{1, 11, 37, 407\}$.
Por otro lado, como $\operatorname{mcm}(a, b) \operatorname{mcd}(a, b) = ab$, tenemos

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

Por lo tanto

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

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

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

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

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

$$ax + by = c$$

tiene solución si y solo si $\operatorname{mcd}(a, b) \mid c$.
Solución: Sea $d = \operatorname{mcd}(a, b)$. Como $(a, b) \neq (0, 0)$ tenemos que $d \neq 0$.

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

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

Ejercicio 3.

a. Hallar el menor x natural que verifica

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

b. Si $(n, e) = (1339, 311)$ calcular $E(11)$, donde E es la función de cifrado del criptosistema RSA con clave pública (n, e).

c. Sabiendo que $1339 = 13 \cdot 103$ calcular la función de descifrado D del criptosistema RSA para la clave pública (n, e) de la parte anterior.

d. Sean $n = p \cdot q$, con p, q primos, y $0 < e < \varphi(n)$ con $\operatorname{mcd}(e, \varphi(n)) = 1$. Dadas las funciones de cifrado E y descifrado D del criptosistema RSA para (n, e), probar que $D(E(x)) \equiv x \pmod{n}$ cuando $\operatorname{mcd}(x, n) = 1$.

Solución:

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

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

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

$$x = 474.$$

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

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

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

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

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

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

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

$$E(x) = 474.$$

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

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

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

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

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

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

Entonces

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

Ejercicio 4. Demostrar la siguiente versión del teorema chino del resto.
Sean m_1, m_2 enteros coprimos y a_1, $a_2 \in \mathbb{Z}$, entonces el sistema

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

tiene solución y es única módulo $m_1 m_2$.

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

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

o lo que es lo mismo

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

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

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

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

Primer parcial - 27 de abril de 2017. Duración: 3 horas

N° de parcial	Cédula	Apellido y nombre	Horario muestra

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

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

$$ax + by = c$$

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

Ejercicio 3.

a. Hallar el menor x natural que verifica

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

b. Si $(n, e) = (1339, 311)$ calcular $E(11)$, donde E es la función de cifrado del criptosistema RSA con clave pública (n, e).

c. Sabiendo que $1339 = 13 \cdot 103$ calcular la función de descifrado D del criptosistema RSA para la clave pública (n, e) de la parte anterior.

d. Sean $n = p \cdot q$, con p, q primos, y $0 < e < \varphi(n)$ con $\text{mcd}(e, \varphi(n)) = 1$. Dadas las funciones de cifrado E y descifrado D del criptosistema RSA para (n, e), probar que $D(E(x)) \equiv x \pmod{n}$ cuando $\text{mcd}(x, n) = 1$.

Ejercicio 4. Demostrar la siguiente versión del teorema chino del resto.
Sean m_1, m_2 enteros coprimos y a_1, $a_2 \in \mathbb{Z}$, entonces el sistema

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

tiene solución y es única módulo $m_1 m_2$.

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

Solución primer prueba
9 de setiembre de 2016

Ejercicio 1.

a. Resolver la ecuación diofántica:

$$738x + 621y = 45$$

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

Solución:

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

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

Tenemos:

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

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

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

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

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

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

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

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

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

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

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

Ejercicio 2. Sea $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ con p_i primos distintos y $\alpha_i \in \mathbb{Z}^+$.
Demostrar que n es un cuadrado perfecto si y solo si el número de divisores positivos de n es impar.

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

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

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

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

Solución segunda prueba (primer parcial) - 30 de setiembre de 2016.

Ejercicio 1. (8 puntos) Calcular $3^{163} \pmod{89}$.

Solución: Observar primero que $3^{163} = 3^{88}3^{75}$. Como $\mathrm{mcd}(89,3) = 1$ (obsérvese que 89 es primo), entonces $3^{88} \equiv 1 \pmod{89}$, por el teorema de Fermat o de Euler. Entonces $3^{163} \equiv 3^{75} \pmod{89}$. Para calcular $3^{75} \pmod{89}$ usaremos el método de exponenciación rápida. Para eso obsérvese que: $75 = 64 + 8 + 2 + 1 = 2^6 + 2^3 + 2^1 + 2^0$.

Planteamos la tabla:

n	$3^{2^n} \pmod{89}$
0	3
1	9
2	$81 \equiv -8$
3	$64 \equiv -25$
4	$625 \equiv 2$
5	4
6	16

Entonces $3^{163} \equiv 3^{75} \pmod{89} \equiv 3^{2^6}3^{2^3}32^1 3^{2^0} \pmod{89} \equiv 16 \times 64 \times 9 \times 3 \pmod{89} \equiv 32 \times 3 \times 32 \times 3 \times 3 \pmod{89} \equiv 7 \times 7 \times 3 \pmod{89} \equiv 58 \pmod{89}$.
Finalmente se obtiene que $3^{163} \equiv 58 \pmod{89}$.

Ejercicio 2. (8 puntos) Sea $a, b, c, n \in \mathbb{N}$ con $c \neq 0$.
Demostrar que, si $ca \equiv cb \pmod{n}$ entonces $a \equiv b \left(\text{ mód } b \ \frac{n}{\mathrm{mcd}(c,n)} \right)$.
Solución: (esto es parte del teórico, página 27, Proposición 2.2.4 del Capítulo 2).
Si llamamos $d = \mathrm{mcd}(c, n)$ tenemos que $c = dc^*$ y $n = dn^*$, con c^*, n^* enteros coprimos. Si $ca \equiv cb \pmod{n}$, entonces $dc^*a \equiv dc^*b \pmod{dn^*}$,con lo cual se obtiene que $c^*a \equiv c^*b \pmod{n^*}$. Ahora como $\mathrm{mcd}(c^*, n^*) = 1$, se concluye que $a \equiv b \pmod{n^*}$; es decir $a \equiv b \left(\text{mód } \frac{n}{\mathrm{mcd}(c,n)} \right)$.

Ejercicio 3. (14 puntos) Se dice que un entero n es un *Pseudoprimo de Carmichael* si n es compuesto y $a^n \equiv a \pmod{n}$ para todo $a \in \mathbb{N}$.

a. Sea b un número entero positivo y coprimo con 561.

i) Demostrar que $b^2 \equiv 1 \pmod{3}$, $b^{10} \equiv 1 \pmod{11}$ y $b^{16} \equiv 1 \pmod{17}$.

ii) Hallar $b^{560} \pmod{3}$, $b^{560} \pmod{11}$ y $b^{560} \pmod{17}$.

iii) Probar que 561 es un Pseudoprimo de Carmichael (*Sug: hallar* b^{561} *dependiendo si* b *es coprimo o no con* 561).

b. Sea n compuesto y libre de cuadrados (no es divisible por ningún cuadrado), tal que todo divisor primo p de n cumple que $p - 1 | n - 1$. Probar que n es un pseudoprimo de Carmichael.

Solución:

a. i) Como $\mathrm{mcd}(b, 561) = 1$ y $561 = 3 \times 11 \times 17$ (descomposición en factores primos), entonces $\mathrm{mcd}(b, 3) = 1$, $\mathrm{mcd}(b, 11) = 1$, $\mathrm{mcd}(b, 17) = 1$. Luego, por el Teorema de Fermat tenemos que: $b^2 \equiv 1 \pmod{3}$, $b^{10} \equiv 1 \pmod{11}$ y $b^{16} \equiv 1 \pmod{17}$.

ii) Observemos para este punto que 560 se puede escribir de las siguientes formas: $560 = 2 \times 280 = 10 \times 56 = 16 \times 35$.
Entonces $b^{560} = (b^2)^{280} \equiv (1)^{280} \pmod{3}$, pues, por el punto anterior $b^2 \equiv 1 \pmod{3}$. También $b^{560} = (b^{10})^{56} \equiv (1)^{56} \pmod{11}$, pues, por el punto anterior $b^{10} \equiv 1 \pmod{11}$. Finalmente vale también que $b^{560} = (b^{16})^{35} \equiv (1)^{35} \pmod{17}$, pues, por el punto anterior $b^{16} \equiv 1 \pmod{17}$.

iii) Si 3 no divide a b entonces $b^2 \equiv 1 \pmod 3$, por lo tanto $b^{560} = (b^2)^{280} \equiv (1)^{280} \pmod 3$. O sea que $b^{560} \equiv 1 \pmod 3$ y por lo tanto $b^{561} \equiv b \pmod 3$.
Si 3 divide a b entonces es claro que $b^{561} - b$ es múltiplo de 3. O sea que también vale $b^{561} \equiv b \pmod 3$.
Conclusión, en ambos casos vale que $b^{561} \equiv b \pmod 3$.

Si 11 no divide a b entonces $b^{10} \equiv 1 \pmod{11}$, por lo tanto $b^{560} = (b^{10})^{56} \equiv (1)^{56} \pmod{11}$. O sea que $b^{560} \equiv 1 \pmod{11}$ y por lo tanto $b^{561} \equiv b \pmod{11}$.
Si 11 divide a b entonces es claro que $b^{561} - b$ es múltiplo de 11. O sea que también vale $b^{561} \equiv b \pmod{11}$.
Conclusión, en ambos casos vale que $b^{561} \equiv b \pmod{11}$.

Si 17 no divide a b entonces $b^{16} \equiv 1 \pmod{17}$, por lo tanto $b^{560} = (b^{16})^{35} \equiv (1)^{35} \pmod{17}$. O sea que $b^{560} \equiv 1 \pmod{17}$ y por lo tanto $b^{561} \equiv b \pmod{17}$.
Si 17 divide a b entonces es claro que $b^{561} - b$ es múltiplo de 17. O sea que también vale $b^{561} \equiv b \pmod{17}$.
Conclusión, en ambos casos vale que $b^{561} \equiv b \pmod{17}$.

Sumando las conclusiones tenemos que $b^{561} - b$ es múltiplo de 3, de 11 y de 17. Por lo tanto, $b^{561} - b$ es múltiplo de 561. O sea que $b^{561} \equiv b \pmod{561}$, para todo $b \in \mathbb{N}$.

b. Seguiremos el mismo proceso de discusión que en el caso anterior. Sea p un primo de la descomposición factorial de n y consideramos $b \in \mathbb{N}$.
Si p no divide a b entonces $b^{p-1} \equiv 1 \pmod p$. Por hipótesis, $p - 1 | n - 1$ o sea que existe k tal que $k \times (p - 1) = n - 1$. Luego $(b^{p-1})^k \equiv (1)^k \pmod p \equiv 1 \pmod p$. O sea que $b^{n-1} \equiv 1 \pmod p$, por lo tanto $b^n \equiv b \pmod p$.
Por otro lado si p divide a b es claro que: $b^n \equiv b \pmod p$. Entonces en ambos casos tenemos la misma conclusión.

Como lo anterior es cierto para cada primo que divide a n, y $n = p_1 \times p_2 \times ... \times p_k$, con $p_i \neq p_j$, si $i \neq j$ (n es libre de cuadrados) y $b^n \equiv b \pmod{p_i}$, para todo $i = 1, ..., k$ entonces $b^n \equiv b \pmod n$.

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

Primer prueba - 9 de setiembre de 2016. Duración: 60 - 90 minutos

N° de parcial	Cédula	Nombre y apellido

Ejercicio 1.

a. Resolver la ecuación diofántica:

$$738x + 621y = 45$$

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

Ejercicio 2. Sea $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ con p_i primos distintos y $\alpha_i \in \mathbb{Z}^+$.
Demostrar que n es un cuadrado perfecto si y solo si el número de divisores positivos de n es impar.

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

Primer prueba - 9 de setiembre de 2016. Duración: 60 - 90 minutos

N° de parcial	Cédula	Nombre y apellido

Ejercicio 1.

a. Resolver la ecuación diofántica:

$$738x + 621y = 45$$

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

Ejercicio 2. Sea $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ con p_i primos distintos y $\alpha_i \in \mathbb{Z}^+$.
Demostrar que n es un cuadrado perfecto si y solo si el número de divisores positivos de n es impar.

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

Segunda prueba (primer parcial) - 30 de setiembre de 2016. Duración: 2,5 horas

N° de parcial	Cédula	Nombre y apellido

Ejercicio 1. (8 puntos) Calcular $3^{163} \pmod{89}$.

Ejercicio 2. (8 puntos) Sea $a, b, c, n \in \mathbb{N}$ con $c \neq 0$.
Demostrar que, si $ca \equiv cb \pmod{n}$ entonces $a \equiv b \left(\text{mód } \frac{n}{\text{mcd}(c,n)}\right)$.

Ejercicio 3. (14 puntos) Se dice que un entero n es un *Pseudoprimo de Carmichael* si n es compuesto y $a^n \equiv a \pmod{n}$ para todo $a \in \mathbb{N}$.

a. Sea b un número entero positivo y coprimo con 561.

- **i**) Demostrar que $b^2 \equiv 1 \pmod{3}$, $b^{10} \equiv 1 \pmod{11}$ y $b^{16} \equiv 1 \pmod{17}$.
- **ii**) Hallar $b^{560} \pmod{3}$, $b^{560} \pmod{11}$ y $b^{560} \pmod{17}$.
- **iii**) Probar que 561 es un Pseudoprimo de Carmichael (*Sug: hallar* b^{561} *dependiendo si* b *es coprimo o no con* 561).

b. Sea n compuesto y libre de cuadrados (no es divisible por ningún cuadrado), tal que todo divisor primo p de n cumple que $p-1|n-1$. Probar que n es un pseudoprimo de Carmichael.

Sugerencia: para cada $a \in \mathbb{N}$ *escribir* $n = n^* d_a$, *siendo* $d_a =$mcd(a, n).

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

Primer parcial - 5 de mayo de 2016. Duración: 3 horas

Ejercicio 1.

a. Calcular el inverso de 5 módulo 121.

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

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

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

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

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

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

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

Solución: Usando el Teorema Chino, tenemos:

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

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

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

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

Ejercicio 2. Dado el sistema

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

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

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

Ejercicio 3.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

PRIMER PRUEBA - 11 DE SSETIEMBRE DE 2015. DURACIÓN: 1 HORA Y MEDIA

Primer prueba - soluciones

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

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

Mostrar el procedimiento para llegar a su respuesta.

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

$$46x + 26y = 600$$

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

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

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

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

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

Multiplicando por 300 obtenemos que

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

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

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

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

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

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

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

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

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

Escribimos las descomposiciones factoriales de a y b:

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

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

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

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

si y sólo si

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

Entonces tenemos que se debe cumplir que

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

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

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

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

Es decir, si y sólo si

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

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

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

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

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

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

- La condición $1 + 3a_2 = 2b_2$ implica que a_2 es impar; es decir $a_2 = 2c_2 + 1$ para algún $c_2 \in \mathbb{N}$; y luego $2b_2 = 1 + 3(2c_2 + 1) = 6c_2 + 4$ y entonces $b_2 = 3c_2 + 2$.

- La condición $3a_3 = 3 + 2b_3$ implica que $2b_3 = 3a_3 - 3 = 3(a_3 - 1)$. Por lo tanto $3 \mid 2b_3$, y como $\mathrm{mcd}(2, 3) = 1$, por el Lema de Euclides tenemos que $3 \mid b_3$; por lo tanto, $b_3 = 3c_3$ para algún $c_3 \in \mathbb{N}$. Y despejando a_3 obtenemos que $a_3 = 1 + 2c_3$.

- La condición $2 + 3a_5 = 2b_5$ implica que $3a_5 = 2b_5 - 2 = 2(b_5 - 1)$ y por lo tanto $2 \mid 3a_5$ y nuevamente por el Lema de Euclides tenemos que se $2 \mid a_5$. Entonces $a_5 = 2c_5$ para algún $c_5 \in \mathbb{N}$. Y despejando b_5 obtenemos que $b_5 = 1 + 3c_5$.

- La condición $3a_p = 2b_p$ para $p \neq 2, 3, 5$, implica que (por el Lema de Euclides nuevamente) $2 \mid a_p$, es decir que $a_p = 2c_p$ para algún $c_p \in \mathbb{N}$. Y despejando b_p obtenemos que $b_p = 3c_p$.

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

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

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

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

PRIMER PARCIAL - 30 DE SETIEMBRE DE 2015.
Solución.

Ejercicio 1.

a. Enunciar el Teorema de Euler.

Ver notas teóricas: Teorema 2.6.5 en la página 40.

b. Calcular las siguientes potencias.

i) $3^{100} \pmod{104}$. Como $104 = 2^3 13$ entonces $\varphi(104) = 2^2 12 = 48$. Para calcular la potencia podemos utilizar el teorema de Euler ya que 3 y 104 son coprimos, con lo que nos queda

$$3^{100} = 3^{48\cdot 2+4} = \left(3^{48}\right)^2 3^4 \equiv 3^4 \pmod{104} \equiv 81 \pmod{104}.$$

ii) $10^{97} \pmod{101}$. En este caso también podemos aplicar el teorema de Euler ya que 101 es primo. Como 101 es primo $\varphi(101) = 100$ y $10^{97} \equiv 10^{-3} \pmod{101} \equiv \left(10^{-1}\right)^3 \pmod{101}$.

Tenemos que calcular $10^{-1} \pmod{101}$, y para esto observamos que $10 \cdot 10 = 100 \equiv -1 \pmod{101}$ entonces $10 \cdot (-10) \equiv 1 \pmod{101}$ y concluimos que $10^{-3} \equiv (-10)^3 \pmod{101} \equiv (-1000) \pmod{101} \equiv 10 \pmod{101}$.

iii) $6^{66} \pmod{99}$.

En este caso no podemos aplicar el teorema de Euler dado que $6 = 2 \cdot 3$ y $99 = 3^2 \cdot 11$ no son coprimos. Lo que podemos hacer es aplicar el teorema chino del resto de la siguiente manera:

$$x \equiv 6^{66} \pmod{99} \Leftrightarrow \begin{cases} x \equiv 6^{66} \pmod{9} \\ x \equiv 6^{66} \pmod{11} \end{cases} \Leftrightarrow \begin{cases} x \equiv 0 \pmod{9} \\ x \equiv 6^{6} \pmod{11} \end{cases}.$$

Calculamos $6^6 \pmod{11}$ que es 5. La solución del sistema es 27 y entonces $6^{66} \equiv 27 \pmod{101}$.

Aclaración: cuando pedimos calcular $a^m \pmod{n}$, nos referimos a hallar $x \in \mathbb{N}$, con $0 \leq x < n$ tal que $a^m \equiv x \pmod{n}$

Ejercicio 2.

a. Sean a, b y c enteros no nulos tales que $\operatorname{mcd}(a, b) \mid c$. Consideramos la ecuación diofántica

$$ax + by = c$$

y (x_0, y_0) una solución particular de la misma.

i) Probar que para todo $k \in \mathbb{Z}$ el par

$$\left(x_0 + k\frac{b}{\operatorname{mcd}(a,b)}, y_0 - k\frac{a}{\operatorname{mcd}(a,b)}\right)$$

también es solución de la ecuación.

ii) Probar que todas las soluciones de la ecuación son de la forma

$$\left(x_0 + k\frac{b}{\operatorname{mcd}(a,b)}, y_0 - k\frac{a}{\operatorname{mcd}(a,b)}\right).$$

Es decir, probar que si (x_1, y_1) es solución de la ecuación, entonces existe $k \in \mathbb{Z}$ tal que

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

La solución de ambas partes es el Teorema 1.5.3 de las notas teóricas en la página 17.

b. i) Hallar todas las soluciones módulo 41 de la ecuación $4x \equiv 7 \pmod{41}$.
Como 4 es invertible módulo 41 hay una sola solución a la congruencia que será $x \equiv 4^{-1} \cdot 7 \pmod{41}$. Como $4 \cdot 10 \equiv -1 \pmod{41}$ y $4^{-1} \equiv -10 \pmod{41} \equiv 31$. Por lo tanto $x \equiv 7 \cdot -10 \pmod{41} \equiv -70 \pmod{41} \equiv 12 \pmod{41}$.

ii) Hallar todas las soluciones módulo 80 de la ecuación $25x \equiv 10 \pmod{80}$.
En este caso no podemos hacer lo mismo que en el caso anterior dado que 25 no es invertible módulo 80. Pero la congruencia anterior es equivalente a la diofántica

$$25x + 80y = 10,$$

que claramente tiene solución dado que $\mathrm{mcd}(25, 80) = 5 \mid 10$. Una solución particular es $(-6, 2)$ encontrada utilizando el Algoritmo Extendido de Euclides. Esto implica que todas las soluciones de x son de la forma

$$-6 + \frac{80}{5}k = -6 + 16k.$$

Y como nos interesa los x módulo 80 vemos que las soluciones son $x \equiv -6+16k \pmod{80}$ con $k = 0, 1, 2, 3, 4$. Las calculamos y dan

$$x \equiv 10, 26, 42, 58, 74 \pmod{80}.$$

Ejercicio 3. Para cada uno de los siguientes sistemas, investigar si tiene solución, y en caso que tenga solución, hallar todas todas sus soluciones.

a. $\begin{cases} x \equiv 7 \pmod{11} \\ x \equiv 13 \pmod{20} \\ x \equiv 14 \pmod{21} \end{cases}.$ **b.** $\begin{cases} x \equiv 7 \pmod{22} \\ x \equiv 21 \pmod{28} \\ x \equiv 23 \pmod{30} \end{cases}.$

a. Dado que los módulos del sistema son coprimos 2 a 2 sabemos que el sistema tiene solución por el Teorema Chino del Resto. Utilizamos el método dado en el ejercicio 4 del práctico 5 para su resolución, pero antes aplicamos un cambio de variable lineal para facilitar las cuentas. Si definimos $x' = x + 7$, entonces el nuevo sistema a resolver es

$$\begin{cases} x' \equiv 3 \pmod{11} \\ x' \equiv 0 \pmod{20} \\ x' \equiv 0 \pmod{21} \end{cases}.$$

Ahora, la solución al sistema viene dada por $x' \equiv 3b_1M_1 + 0b_2M_2 + 0b_3M_3 \pmod{11 \cdot 20 \cdot 21}$, donde b_i es el inverso de M_i módulo m_i. m_i son los módulos y M_i es el producto de todos los módulos menos el i-ésimo. Entonces solo tenemos que calcular el inverso de $M_1 = 20 \cdot 21$ módulo 11. Ahora $20 \cdot 21 \equiv (-2) \cdot (-1) \pmod{11} \equiv 2 \pmod{11}$ y $M_1^{-1} \equiv 6 \pmod{11}$. Por lo tanto la sólucion al sistema con x' es $3 \cdot 6 \cdot 20 \cdot 21 = 7560 \equiv 2940 \pmod{11 \cdot 20 \cdot 21}$. Concluimos que $x \equiv 2933 \pmod{11 \cdot 20 \cdot 21}$.

b. Aplicando el TCR a cada una de las congruencias vemos que

$$\begin{cases} x \equiv 7 \pmod{22} \\ x \equiv 21 \pmod{28} \\ x \equiv 23 \pmod{30} \end{cases} \Leftrightarrow \begin{cases} x \equiv 7 \pmod{11} \\ x \equiv 7 \pmod{2} \\ x \equiv 21 \pmod{4} \\ x \equiv 21 \pmod{7} \\ x \equiv 23 \pmod{2} \\ x \equiv 23 \pmod{3} \\ x \equiv 23 \pmod{5} \end{cases} \Leftrightarrow \begin{cases} x \equiv 7 \pmod{11} \\ x \equiv 1 \pmod{2} \\ x \equiv 1 \pmod{4} \\ x \equiv 0 \pmod{7} \\ x \equiv 1 \pmod{2} \\ x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \end{cases}.$$

Como $x \equiv 1 \pmod{4}$ implica $x \equiv 1 \pmod{2}$ vemos que el sistema es equivalente a

$$\begin{cases} x \equiv 7 \pmod{11} \\ x \equiv 1 \pmod{4} \\ x \equiv 0 \pmod{7} \\ x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \end{cases}.$$

Aplicando TRC a las congruencias 2 y 5 vemos que

$$\left\{\begin{array}{lll} x & \equiv & 1 \pmod{4} \\ x & \equiv & 3 \pmod{5} \end{array}\right. \Leftrightarrow x \equiv 13 \pmod{20},$$

y lo mismo para las ecuaciones 3 y 4 para obtener

$$\left\{\begin{array}{lll} x & \equiv & 0 \pmod{7} \\ x & \equiv & 2 \pmod{3} \end{array}\right. \Leftrightarrow x \equiv 14 \pmod{21}.$$

Por lo que el sistema queda equivalente al de la parte anterior y tiene la misma solución.

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

PRIMER PRUEBA - 11 DE SETIEMBRE DE 2015. DURACIÓN: 1.5 HORAS

N° de parcial	Cédula	Apellido y nombre

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

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

Mostrar el procedimiento para llegar a su respuesta.

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

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

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

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

Primer parcial - 30 de setiembre de 2015. Duración: 3 horas

N° de parcial	Cédula	Apellido y nombre

Ejercicio 1.

a. Enunciar el Teorema de Euler.

b. Calcular las siguientes potencias.

i) $3^{100} \pmod{104}$.
ii) $10^{97} \pmod{101}$.
iii) $6^{66} \pmod{99}$.

Aclaración: cuando pedimos calcular $a^m \pmod{n}$*, nos referimos a hallar* $x \in \mathbb{N}$*, con* $0 \leq x < n$ *tal que* $a^m \equiv x \pmod{n}$

Ejercicio 2.

a. Sean a, b y c enteros no nulos tales que $\operatorname{mcd}(a,b) \mid c$. Consideramos la ecuación diofántica

$$ax + by = c$$

y (x_0, y_0) una solución particular de la misma.

i) Probar que para todo $k \in \mathbb{Z}$ el par

$$\left(x_0 + k\frac{b}{\operatorname{mcd}(a,b)}, y_0 - k\frac{a}{\operatorname{mcd}(a,b)}\right)$$

también es solución de la ecuación.

ii) Probar que todas las soluciones de la ecuación son de la forma

$$\left(x_0 + k\frac{b}{\operatorname{mcd}(a,b)}, y_0 - k\frac{a}{\operatorname{mcd}(a,b)}\right).$$

Es decir, probar que si (x_1, y_1) es solución de la ecuación, entonces existe $k \in \mathbb{Z}$ tal que

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

b. i) Hallar todas las soluciones módulo 41 de la ecuación $4x \equiv 7 \pmod{41}$.

ii) Hallar todas las soluciones módulo 80 de la ecuación $25x \equiv 10 \pmod{80}$.

Ejercicio 3. Para cada uno de los siguientes sistemas, investigar si tiene solución, y en caso que tenga solución, hallar todas todas sus soluciones.

a. $\begin{cases} x \equiv 7 \pmod{11} \\ x \equiv 13 \pmod{20} \\ x \equiv 14 \pmod{21} \end{cases}$.

b. $\begin{cases} x \equiv 7 \pmod{22} \\ x \equiv 21 \pmod{28} \\ x \equiv 23 \pmod{30} \end{cases}$.

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

Primer parcial - 4 de mayo de 2015. Duración: 3 horas

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

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

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

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

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

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

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

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

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

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

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

que tiene solución 27.

Segunda parte: Desarrollo

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

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

Ver notas de teórico.

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

Ver notas de teórico.

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

Ejercicio 4. Dado el sistema

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

investigar si tiene solución, y en caso que tenga encontrar todas sus soluciones.
Como $56 = 2^3 \cdot 7$, $21 = 3 \cdot 7$, $36 = 2^2 \cdot 3^2$ y $49 = 7^2$, entonces

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

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

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

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

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

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

Ejercicio 5.

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

Si $x^2 \equiv 1 \pmod{p}$ entonces $0 \equiv (x^2 - 1) \pmod{p} \equiv (x-1)(x+1) \pmod{p}$ y $p \mid (x-1)(x+1)$. Ahora, como p es primo $p \mid (x-1)$ o $p \mid (x+1)$, por lo cual

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

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

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

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

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

por lo que

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

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

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

que son las 8 opciones posibles.

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

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

N° de parcial	Cédula	Apellido y nombre	Salón	Teórico

Primera parte: Múltiple Opción

MO	
1	2

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

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

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

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

Segunda parte: Desarrollo

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

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

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

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

Ejercicio 4. Dado el sistema

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

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

Ejercicio 5.

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

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

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

Primer parcial - soluciones

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

Ejercicio 2.

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

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

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

luego el resto buscado es 241.

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

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

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

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

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

Ejercicio 3.

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

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

$$100x - 46y = 1000$$

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

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

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

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

Ejercicio 4.

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

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

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

Dividiendo entre 3 obtenemos:

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

De aquí:

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

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

b) **Investigar si el siguiente sistema tiene solución:**

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

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

c) **Resolver el sistema:**

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

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

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

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

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

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

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

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

Entonces, es suficiente resolver el siguiente sistema:

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

Resolviendo las primeras dos ecuaciones tenemos:

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

luego

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

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

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

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

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

N° de parcial	Cédula	Apellido y nombre	Salón

Primer parcial
(se hace sin material y sin calculadora)

Ejercicio 1. Enunciar y demostrar el Lema de Euclides.

Ejercicio 2.

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

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

Ejercicio 3. Una companía compró cierto número de reliquias falsas a 46 pesos cada una y vendió algunas de ellas a 100 pesos cada una. Si la cantidad comprada originalmente es mayor que 400 pero menor que 500 y la companía obtuvo una ganancia de 1000 pesos, ¿cuántas reliquias no se vendieron?

Ejercicio 4.

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

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

b) Investigar si el siguiente sistema tiene solución:

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

c) Resolver el sistema:

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

Ejercicio 5. Probar que existen infinitos números primos.

Ejercicio 6. Sea ϕ la función de Euler y sean m y $n \in \mathbb{Z}^+$ coprimos. Probar que $\phi(mn) = \phi(m)\phi(n)$. (Si usan alguna fórmula para $\phi(n)$ la tienen que demostrar.)

Ejercicio 1) Sea S_a el sistema de congruencias

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

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

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

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

Y dicho sistema tiene solución si y sólo si el sistema

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

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

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

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

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

El sistema S_a con $a = 11$ queda

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

o lo que es lo mismo

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

El sistema

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

ya fue resuelto en la parte anterior y se concluyó $x \equiv 11 (\text{mod } 21)$.

Luego, resolver S_{11} es resolver

$$\begin{cases} x \equiv 5 & \pmod{11} \\ x \equiv 11 & \pmod{21} \end{cases}$$

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

Ejercicio 2)
a)Dado $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_t^{\alpha_t}$ con $\alpha_i \geq 1$ y p_i primos para todo $i = 1, \ldots, t$, determinar el número de divisores y demostrar el resultado.

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

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

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

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

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

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

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

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

Ejercicio 3)

Sea ϕ la función de Euler.

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

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

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

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

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

b)1) Hallar $d = mcd(m, n)$.

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

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

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

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

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

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

Luego se obtiene lo querido.

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

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