

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

**Ejercicio 1.**

a.

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

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  $1 = \text{mcd}(16, 11) = 11(3) - 16(2)$ ; así 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  $\text{mcd}(a, n) = 1$  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  $\boxed{x \equiv 8 \pmod{11}}$ .

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  $\boxed{x \equiv 11 \pmod{16}}$ .

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

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

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  $a$ ), concluimos 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  $\text{mcd}(a, b) = 1$ .

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

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

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

- 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 descomposición 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 algún 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

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

- b. Llamamos  $a = p_1 p_2 \cdots p_k$ ,  $b = p_{k+1} p_{k+2} \cdots p_n$  y  $c = p_1 p_2 \cdots p_k + p_{k+1} p_{k+2} \cdots p_n = a + b$ . 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  $p_i \mid p_1 p_2 \cdots p_k = a$  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  $c \geq p \geq p_{n+1}$ .