Álgebra 1: Práctica 4

Máximo Común Divisor y Congruencias Módulo m

Viernes 5/5/2023

Máximo Común Divisor: $d > 0$

Propiedades: Sean $a, b, c, m \in \mathbb{Z}$, con $b \neq 0$

- $(a : b) = (-a : b) = (a : -b) = (-a : -b)$
- $(a : b) = (a - k \cdot b : b)$
- Si $a \equiv c \ mod(b) \Rightarrow (a : b) = (c : b)$
- $Si\ a = q \cdot b + r,\ 0 \leq r < b \implies (a : b) = (r : b)$
- $(ma : mb) = m(a : b)$

MCD. Ejercicio 1

Calcular los valores posibles del máximo común divisor

$$d := (3n+5 : 8n-1) : \ n \in \mathbb{Z}$$

Exhibir un n para cada uno de ellos.

Solución: Sea $d := (3n+5 : 8n-1)$

$$\Longrightarrow \left\{ \begin{array}{ll} d \Big| (3n+5) & \Longrightarrow d \Big| \underbrace{8 \cdot (3n+5)}_{=24n+40} \\ & \\ d \Big| (8n-1) & \Longrightarrow d \Big| \underbrace{3 \cdot (8n-1)}_{=24n-3} \end{array} \right\} \Longrightarrow d \Big| 43$$

$\Longrightarrow d = 1 \vee d = 43$ pues 43 es primo ✓

¿Vale siempre $d = 1$?

- Si $n = 0 \Longrightarrow d = (5 : -1) = 1$
- Si $n = 1 \Longrightarrow d = (8 : 7) = 1$
- Si $n = 2 \Longrightarrow d = (11 : 15) = 1$
- Si $n = 3 \Longrightarrow d = (14 : 23) = 1$, etc.

MCD. Ejercicio 2

Calcular el máximo común divisor

$$d := (3n+5 : 8n-1): \text{ para cada } n \in \mathbb{Z}$$

Solución: $d := (3n+5 : 8n-1) = (a : b) = (a : b-3a)$

$$= (3n+5 : 8n-1-3(3a+5)) = (3n+5 : \underbrace{8n-1-9n-15)}_{=-n-16})$$

$$= (3n+5 : n+16)$$

$$= (\underbrace{3n+5-3(n+16)}_{=-43} : n+16)$$

$= (43 : n+16) \Longrightarrow d = 1 \vee d = 43$ pues 43 es primo

¿Para qué $n \in \mathbb{Z}$ vale $d = 43$?

$$d = (43 : n + 16) = 43 \iff 43 \mid (n + 16)$$

$$\iff (n + 16) \equiv 0 \ mod \ 43$$

$$\iff n \equiv -16 \equiv 27 \ mod \ 43$$

$$\iff n = 43 \cdot q + 27$$

Por lo tanto,

$$d = \begin{cases} 43 & si \ n = 43 \cdot q + 27, \ q \in \mathbb{Z} \\ \\ 1 & si \ n \not\equiv 27 \ mod \ 43 \ \checkmark \end{cases}$$

Efectivamente:

- Si $n = 27 \Longrightarrow d = (3n + 5 : 8n - 1) = (86 : 215)$

$$= (43 \cdot 2 : 43 \cdot 5)$$

$$= 43 \cdot \underbrace{(2 : 5)}_{=1}$$

$$= 43 \checkmark$$

MCD. Ejercicio 3

Calcular el máximo común divisor $(18 : 174)$ y escribirlo como combinación lineal en $\mathbb{Z}$.

Solución: Recordemos la propiedad
$(ma : mb) = m(a : b)\ \forall\ m, a, b \in \mathbb{Z}$

Calculemos $174 = 2 \cdot 3 \cdot 29$ entonces

$$(18 : 174) = (2 \cdot 3^2 : 2 \cdot 3 \cdot 29) = 2 \cdot 3\underbrace{(3 : 29)}_{=1} = 6$$

$$\Longrightarrow (18 : 174) = 6$$

Combinación lineal

Usemos otra propiedad: $(a : b) = (a : r)$ si $b = a \cdot q + r$
Dividamos el más grande por el más chico y seguimos así dividiendo por los sucesivos restos:

- $174 = 9 \cdot 18 + 12 \quad \Longrightarrow \quad (18 : 174) = (18 : 12)$
- $18 = 1 \cdot 12 + 6 \quad \Longrightarrow \quad (18 : 12) = (12 : 6)$
- $12 = 1 \cdot 2 + 0 \quad \Longrightarrow \quad (12 : 6) = 6$

Luego, recuperamos la combinación lineal recorriendo hacia atrás las igualdades anteriores:

$$6 = 18 - 12 \; = 18 - \Big[\underbrace{174 - 9 \cdot 18}_{=12}\Big]$$

$$= 18 \cdot \Big[1 + 9\Big] - 174$$

$$\Longrightarrow 6 = 18 \cdot 10 - 174 \cdot 1 \; \checkmark$$

Ejercicio 4. a) Calcular todos los posibles valores de

$$d := (7^{n-1} + 5^{n+2} : 5 \cdot 7^n - 5^{n+1})$$

Solución: Usemos la propiedad $(a : b) = (a : b + ka)$

$$\Longrightarrow d = \left(7^{n-1} + 5^{n+2} : \underbrace{5 \cdot 7^n}_{\text{cancelemos éste}} - 5^{n+1}\right)$$

$$= \left(7^{n-1} + 5^{n+2} : 5 \cdot 7^n - 5^{n+1} - (5 \cdot 7 \cdot (7^{n-1} + 5^{n+2}))\right)$$

$$= \left(7^{n-1} + 5^{n+2} : \cancel{5 \cdot 7^n} - 5^{n+1} - \cancel{5 \cdot 7^n} - 7 \cdot 5^{n+3}\right)$$

$$= \left(7^{n-1} + 5^{n+2} : -5^{n+1} - 7 \cdot 5^{n+3}\right)$$

$$= \left(7^{n-1} + 5^{n+2} : -\underbrace{(1 + 7 \cdot 5^2)}_{=176} 5^{n+1}\right)$$

Propiedad: Si $(a : m) = 1 \Longrightarrow (a : mb) = (a : b)$

$$\Longrightarrow d = \Big(\underbrace{7^{n-1} + 5^{n+2}}_{\text{no es múltiplo de 5}} : 176 \cdot 5^{n+1} \Big)$$

$$= \Big(7^{n-1} + 5^{n+2} : 176\Big)$$

$$\Longrightarrow d | 176$$

Además,

$$176 = 16 \cdot 11 = 2^4 \cdot 11$$

Por lo tanto, sus valores posibles son los divisores de 176:

$$d \in \{1,\ 2,\ 4,\ 8,\ 16,\ 11,\ 22,\ 44,\ 88,\ 176\}$$ ✓

Ejemplos con los primeros n

- $n = 1 \Longrightarrow d = (126 : 10) = 2$
- $n = 2 \Longrightarrow d = (632 : 120) = (2^3 \cdot 79 : 2^3 \cdot 3 \cdot 5) = 8$
- $n = 3 \Longrightarrow d = (4350 : 7950) = (2^3 \cdot 3 \cdot 23^2 : 2 \cdot 5 \cdot 109) = 2$
- $n = 4 \Longrightarrow d = (2^5 \cdot 499 : 2^4 \cdot 3 \cdot 5 \cdot 37) = 16$
- $n = 5 \Longrightarrow d = (2 \cdot 3 \cdot 13421 : 2 \cdot 5 \cdot 6841) = 2$

Notar que d es par

$$\Longrightarrow d \in \{\cancel{1},\ 2,\ 4,\ 8,\ 16,\ \cancel{11},\ 22,\ 44,\ 88,\ 176\}$$

Para saber más, habría que estudiar la congruencia módulo 4, 8, 16, 11

b) Probar que si n es par $\Longrightarrow 8|d$ y que si n es impar $\Longrightarrow 2|d$ pero $4 \not| d$.

Solución b) Llamemos $d = (A : B) \Longrightarrow 2|$ ambos $\Longrightarrow 2|d$

- Notar que $7 \equiv -1 \ mod\ 4, \quad 5 \equiv 1 \ mod\ 4$, entonces

$$\begin{cases} A = 7^{n-1} + 5^{n+2} & \equiv (-1)^{n-1} + 1 \equiv 0 \ mod\ 4 \iff n \ par \\ B = 5 \cdot 7^n - 5^{n+1} & \equiv (-1)^n - 1 \equiv 0 \ mod\ 4 \iff n \ par \end{cases}$$

Por otra parte,

$$\begin{cases} A = 7^{n-1} + 5^{n+2} & \equiv (-1)^{n-1} + 1 \equiv 2 \ mod\ 4 \iff n \ impar \\ B = 5 \cdot 7^n - 5^{n+1} & \equiv (-1)^n - 1 \equiv 2 \ mod\ 4 \iff n \ impar \end{cases}$$

Por lo tanto,

- Si n es par $\Longrightarrow 4|$ ambos $\Longrightarrow 4|d$

- Si n es impar $\Longrightarrow 2|$ ambos $\Longrightarrow 2|d$ pero $\Longrightarrow 4 \not| d$

Congruencia módulo 8 para n par

Sea n de la forma $n = 2k$:

$$7 \equiv_8 -1, \quad 5 \equiv_8 -3$$

$$\Rightarrow A = 7^{n-1} + 5^{n+2} \equiv_8 (-1)^{n-1} + (-3)^{n+2} = -(-1)^n + 9(-3)^n$$

$$\equiv_8 -(-1)^{2k} + (-3)^{2k} \equiv_8 -1 + 9^k \equiv_8 -1 + 1 \equiv 0 \ mod\ 8$$

$$\Longrightarrow 8|d$$

Concluímos que

- Si n es par $\Longrightarrow 8|d$

- Si n es impar $\Longrightarrow 2|d$ pero $\Longrightarrow 4 \not| d$

Por lo tanto,

$$\Longrightarrow d \in \{\cancel{1}, 2, \cancel{4}, 8, 16, \cancel{11}, 22, \cancel{44}, 88, 176\}$$ ✓

Item adicional c) Hallar los n: $d = 88$ ó 176. Deducir el valor de d para n impar

Para ver la congruencia módulo 11 consideremos la sgte tabla:

n	7^{n-1}	5^{n+2}	$7^{n-1} + 5^{n+2}$
1	$7^0 = 1$	$5^3 \equiv 125 \equiv 4$	$1 + 4 = 5$
2	$7^1 = 7$	$5^4 \equiv 5 \cdot 4 = 20 \equiv -2$	$7 - 2 = 5$
3	$7^2 = 49 \equiv 5$	$5^5 \equiv 5 \cdot (-2) = -10 \equiv 1$	$5 + 1 = 6$
4	$7^3 \equiv 7 \cdot 5 = 35 \equiv 2$		
5	$7^4 \equiv 7 \cdot 2 = 14 \equiv 3$		
6	$7^5 \equiv 7 \cdot 3 = 21 \equiv -1$		

Notar

$$7^5 \equiv_{11} (-1) \Rightarrow 7^{10} \equiv (-1)^2 = 1 \ mod\ 11$$

También

$$5^5 \equiv_{11} 1 \Rightarrow 5^{10} \equiv 1 \ mod\ 11$$

$\Longrightarrow$ veamos la tabla de $7^{n-1} + 5^{n+2}$ para $n = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10$ y los valores se repiten cada 10.

Tabla de las potencias de 7 y de 5 mod 11

n	7^n	7^{n-1}	5^n	5^{n+2}	$A = 7^{n-1} + 5^{n+2}$
1	7	1	5	4	$1+4=5$
2	$49 \equiv 5$	7	$25 \equiv 3$	-2	$7-2=5$
3	$35 \equiv 2$	5	$15 \equiv 4$	1	$5+1=6$
4	$14 \equiv 3$	2	$20 \equiv -2$	5	$2+5=7$
5	$21 \equiv -1$	3	$-10 \equiv 1$	3	$3+3=6$
6	-7	-1	5	4	$-1+4=3$
7	-5	-7	3	-2	$-7-2=-9$
8	-2	-5	4	1	$-5+1=-4$
9	-3	-2	-2	5	$-2+5=3$
10	1	-3	1	3	$3+3=0$

Vemos que para n=10 $\Longrightarrow$ A es múltiplo de 11, y se repite de 10 en 10 entonces $\Longrightarrow 11|d \iff n = 10k$

Valores que efectivamente toma d

- $n = 1 \Longrightarrow d = (126 : 10) = 2$
- $n = 2 \Longrightarrow d = (632 : 120) = (2^3 \cdot 79 : 2^3 \cdot 3 \cdot 5) = 8$
- $n = 3 \Longrightarrow d = (4350 : 7950) = (2^3 \cdot 3 \cdot 23^2 : 2 \cdot 5 \cdot 109) = 2$
- $n = 4 \Longrightarrow d = (2^5 \cdot 499 : 2^4 \cdot 3 \cdot 5 \cdot 37) = 16$
- $n = 5 \Longrightarrow d = (2 \cdot 3 \cdot 13421 : 2 \cdot 5 \cdot 6841) = 2$
- $n = 10 \Longrightarrow d = 88$
- $n = 20 \Longrightarrow d = 176$

$$\Longrightarrow d \in \{\cancel{1}, 2, \cancel{4}, 8, 16, \cancel{11}, \cancel{22}, \cancel{44}, 88, 176\}$$

Concluímos

- n es múltiplo de 10 entonces $7^{n-1} + 5^{n+2}$ es múltiplo de 8 y de 11, por lo tanto $\Rightarrow d = 88$ ó $d = 176$

- n par pero no múltiplo de 10, entonces $7^{n-1} + 5^{n+2}$ es múltiplo de 8 (pero no de 11) $\Rightarrow d = 8$ ó $d = 16$

- n impar entonces $7^{n-1} + 5^{n+2}$ es par, pero no múltiplo de 4, tampoco múltiplo de 11 $\Rightarrow d = 2$ ✓

Congruencia y algoritmo de la división

$$0 \neq m \in \mathbb{Z}, \quad N \equiv r \ mod(m) \iff m \Big| (N - r)$$

$$\iff N = m \cdot q + r : \ q, r \in \mathbb{Z}$$

Si además $0 \leq r < |m|$

$$\implies r = resto \text{ de la división de } N \text{ por } m$$

Restos usando congruencia

Ejercicio 5.

Calcular el resto de dividir por 4 y por 5 al número

$$N = \sum_{k=400}^{490} k^2$$

Solución: $N \equiv r \ mod(4), 0 \leq r < 4 \Longrightarrow r = resto$

$\Longrightarrow$ *usemos congruencia*

Cálculos auxiliares módulo 4:

- n par $\Longrightarrow n = 2q \Longrightarrow n^2 = 4q^2 \equiv 0 \ mod(4)$

- n impar, $n = 2q + 1$

$$\Longrightarrow n^2 = 4q^2 + 4q + 1 \equiv 1 \ mod(4)$$

$$\Longrightarrow \sum_{k=400}^{490} k^2 = \sum_{k\ par=400}^{490} k^2 + \sum_{k\ impar=401}^{490} k^2$$

$$\equiv 0 + \sum_{k\ impar=401}^{490} 1\ mod(4) \quad \left(* \right)$$

Hay $\dfrac{490-400}{2} = 45$ impares en el conjunto

$$\{400,\ 401,\ \ldots 489,\ 490\}$$

$$\Longrightarrow \left(* \right) \equiv 45 \cdot 1\ mod(4)$$

$$\equiv 1\ mod(4)$$ ✓

Congruencia módulo 5

$$\{400, 401, \ldots, 490\} = \overline{0} \cup \overline{1} \cup \overline{2} \cup \overline{3} \cup \overline{4}$$

$$= \text{ unión disjunta de clases}$$

donde cada clase $\neq \overline{0}$ tiene $\dfrac{490 - 400}{5} = 18$ elementos:

$$\overline{1} = \Big\{401,\ 406,\ 411,\ 416,\ 421,\ 426,\ 431,\ 436,\ 441,\ 446,$$

$$461,\ 456,\ 461,\ 466,\ 471,\ 476,\ 481,\ 486\Big\}$$

$$\Longrightarrow \overline{1} \text{ tiene 18 elementos}$$

En efecto, hay 2 en cada decena y se tienen 9 decenas

Pero

$$\overline{0} = \{400,\ 405,\ 410,\ 415,\ 420,\ 425,\ 430,\ 435,\ 440,\ 445,$$

$$450,\ 455,\ 460,\ 465,\ 470,\ 475,\ 480,\ 485,\ 490\}$$

$$\Longrightarrow \overline{0} \text{ tiene 19 elementos}$$

En efecto, hay 2 en cada decena y se tienen 9 decenas y el 490

Congruencia $\sum_{k=400}^{490} k^2$ de módulo 5

$$\sum_{k=400}^{490} k^2 = \sum_{k\equiv 0} k^2 + \sum_{k\equiv 1} k^2 + \sum_{k\equiv 2} k^2 + \sum_{k\equiv 3} k^2 + \sum_{k\equiv 4} k^2$$

$$\equiv \sum_{k\equiv 0} 0 + \sum_{k\equiv 1} 1^2 + \sum_{k\equiv 2} 2^2 + \sum_{k\equiv 3} 3^2 + \sum_{k\equiv 4} 4^2$$

$$\equiv 18 \cdot \ (1 + 2^2 + 3^2 + 4^2)$$

$$\equiv 18 \cdot \ (1 + 4 + 9 + 16) \equiv 0 \ mod(5)$$ ✓

Ejercicio 6.

a) Calcular el resto de dividir a 8^k por 14 para cada $k \in \mathbb{N}$.
b) Calcular el resto de dividir a 500.000^n por 14 para cada $n \in \mathbb{N}$. ¿De qué depende el resultado?

Solución: a)

- $k = 1 \Longrightarrow 8^1 \equiv 8 \ mod(14)$
- $k = 2 \Longrightarrow 8^2 = 64 = 56 + 8 = 14 \cdot 4 + 8 \equiv 8 \ mod(14)$
- $k = 3 \Longrightarrow 8^3 \equiv 8 \cdot 8^2 \equiv 8 \cdot 8 \equiv 8 \ mod(14)$

Por inducción:

- $8^{k+1} \equiv 8 \cdot 8^k \equiv 8 \cdot 8 \equiv 8 \ mod(14)$

$\Longrightarrow$ Concluímos que $8^k \equiv 8 \ \forall \ k$

$\Longrightarrow 8^k$ tiene resto $r = 8$ en la división por 14, $\forall \ k$ ✓

b) Resto de 500.000^n módulo 14

$$490.000 = 7^2 \cdot 10.000 = 7^2 \cdot 2 \cdot 5.000 = 14 \cdot 35.000 \equiv 0 \ mod(14)$$

$$\begin{aligned}
\Longrightarrow 500.000 &= \underbrace{490.000}_{\equiv 0} + 10.000 \\
&\equiv 10.000 \ mod(14) \\
&\equiv \underbrace{7.000}_{\equiv 0} + 3.000 \ mod(14) \\
&\equiv 3.000 \ mod(14) \\
&\equiv \underbrace{2.800}_{\equiv 0} + 200 \ mod(14) \\
&\equiv \underbrace{140}_{\equiv 0} + 60 \ mod(14) \\
&\equiv 4 \ mod(14)
\end{aligned}$$

Tabla de restos

$$a \equiv b \ mod(14) \Longrightarrow a^n \equiv b^n \ mod(14)$$

$$\Longrightarrow \ 500.000^n \equiv 4^n \ mod(14) \ \forall \ n$$

$\Longrightarrow$ Tabla de restos mod (14) para 4^n

n	4^n	$4^n \ mod \ 14$
1	4	4
2	16	2
3	$16 \cdot 4$	8
4	$2 \cdot 2$	4
5	$4 \cdot 4$	2
6	$2 \cdot 4$	8
7	$8 \cdot 4$	4
		$\ldots$

$\Longrightarrow$ depende de los restos de n módulo 3

Resto de 500.000^n módulo 14

$$n = 3q + r \Longrightarrow \; 500.000^n \equiv 4^n = 4^{3q+r} = \left(4^3\right)^q \cdot 4^r = \left(4^2 \cdot 4\right)^q \cdot 4^r$$

$$\equiv (2 \cdot 4)^q \cdot 4^r \equiv \; 8^q \cdot 4^r$$
$$\equiv 8 \cdot 4^r \; mod \; 14$$

$$\equiv \begin{cases} 8 \cdot 4^0 \equiv 8 \quad si \quad n \quad \equiv 0 \mod 3 \\ 8 \cdot 4^1 \equiv 4 \quad si \quad n \quad \equiv 1 \mod 3 \\ 8 \cdot 4^2 \equiv 2 \quad si \quad n \quad \equiv 2 \mod 3 \; \checkmark \end{cases}$$

Ejercicio 7. Determinar todos los pares $a, b \in \mathbb{Z}$ coprimos: $\frac{b+2}{a} + \frac{7}{b} \in \mathbb{Z}$

Solución: Los pares a, b deben verificar

$$\frac{b(b+2)+7a}{ab} \in \mathbb{Z}$$

$$\iff ab \Big| (b(b+2)+7a)$$

Propiedad: Si $a, b \in \mathbb{Z}$ son coprimos, $m \in \mathbb{Z}$, entonces

$$ab \Big| m \iff a \Big| m \wedge b \Big| m$$

Buscamos todos los pares $a, b \in \mathbb{Z}$ coprimos:

$$\frac{b+2}{a} + \frac{7}{b} \in \mathbb{Z}$$

$\Longrightarrow$ Los pares a, b deben verificar entonces

$$a \Big| (b(b+2)+7a) \wedge b \Big| (b(b+2)+7a)$$

Propiedad: Si $a, b \in \mathbb{Z}$ son coprimos, $m \in \mathbb{Z}$, entonces

$$a \mid b \cdot m \iff a \mid m$$

Tenemos

$$\left.\begin{array}{ll} \bullet a & \mid (b(b+2)+7a) \\ \bullet a & \mid 7a \end{array}\right\} \Longrightarrow a \mid b(b+2) \Longrightarrow a \mid (b+2)$$

Por otra parte,

$$\left.\begin{array}{ll} \bullet b & \mid (b(b+2)+7a) \\ \bullet b & \mid b(b+2) \end{array}\right\} \Longrightarrow b \mid 7a \Longrightarrow b \mid 7$$

$$\Longrightarrow b = \pm 1, \ \pm 7$$

Conclusión: obtenemos los siguientes pares

Usemos la condición $a|(b+2)$:

- Si $b = 1 \Longrightarrow a|3 \Longrightarrow a = \pm 1,\ \pm 3$
- Si $b = -1 \Longrightarrow a|1 \Longrightarrow a = \pm 1$
- Si $b = 7 \Longrightarrow a|9 \Longrightarrow a = \pm 1,\ \pm 3,\ \pm 9$
- Si $b = -7 \Longrightarrow a|(-5) \Longrightarrow a = \pm 1,\ \pm 5$ ✓

Solución: Los pares son

$$(\pm 1, -1),\ (\pm 1, 1),\ (\pm 1, -7),\ (\pm 1, 7),$$

$$(\pm 3, 1),\ (\pm 3, 7),\ (\pm 5, -7),\ (\pm 9, 7)$$ ✓

¡¡¡Buen Viernes!!!

Números Primos y Números Compuestos

Teorema: n es compuesto $\iff$ existe un primo $p|n$ ✓

Lema: n es compuesto $\iff$ existe un primo $p|n$ tal que

$$1 < p \leq \sqrt{n}$$

Dem: $(\Leftarrow)$ es inmediata.

$(\Longrightarrow)$ Dado n compuesto $\Longrightarrow n = m \cdot q$, donde alguno de los dos factores es menor que $\sqrt{n}$, en efecto, si fueran ambos

$$p > \sqrt{n},\ q > \sqrt{n} \Rightarrow n = m \cdot q > \underbrace{\sqrt{n} \cdot \sqrt{n}}_{=n}$$

$$\Longrightarrow n > n, \quad \text{absurdo!}$$

Llamemos q al más chico $\Longrightarrow 1 < q \leq \sqrt{n}$.

- Si q es primo ✓

- Tenemos que $n = m \cdot q$.

Si q no es primo, es compuesto

$$\Longrightarrow \text{ existe un primo } p \Big| q$$

entonces

$$p \Big| q \ \wedge \ q \Big| n \Longrightarrow \ p|n$$

y cumple $1 < p < q \leq \sqrt{n}$ ✓

43 es primo

43 es primo pues no es divisible por ningún primo más chico:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41 ✓