Universidad Carlos III de Madrid
COSEC LAB· Dpto. Informática

Universidad Carlos III de Madrid

Problemas fundamentos matemáticos

ENUNCIADOS

CSI
Curso 2016/2017

Almudena Alcaide Raya

Ejemplos:

$7x = 1 \bmod 12$ $\quad$ $mcd(7,12) = 1$ Coprimos

$x = 7^{-1} \bmod 12$ $\quad$ 12 no primo $\quad 2^2 \cdot 3$

Por Euler:

$\phi(12) = \phi(2^2)\,\phi(3) = 2^1(1)\cdot(2) = 4$

$x = 7^3 \bmod 12 = 7 \cdot 7^2 \bmod 12 = 1 \cdot 7 \bmod 12 = 7 \bmod 12$

$\boxed{x = 7 \bmod 12}$

¿$16^{16} + 16^{17} \bmod 17 = 1 \bmod 17$? No se cumple

$$((\underbrace{16^{16}}_{\substack{(-1)^{16} \\ 1}} \bmod 17) + (\underbrace{16^{17}}_{\substack{(-1)^{17} \\ -1}} \bmod 17)) \bmod 17 = (1-1) \bmod 17 = \underline{0 \bmod 17}$$

¿$16^{16} \times 16^{17} \bmod 17$?

$1 \times -1 \bmod 17$

$-1 \bmod 17 = \underline{16 \bmod 17}$

$32x \bmod 5 = 1$ $\quad$ Por Euclides

$x = 32^{-1} \bmod 5$

$32 = 5 \cdot 6 + 2$

$5 = 2 \cdot 2 + 1$ mcd = 1 coprim aplicable Euclides

$2 = 1 \cdot 2 + 0$

$1 = 5 - 2 \cdot 2$

$1 = 5 - 2 \cdot (32 - 5 \cdot 6) = 5 - 2 \cdot 32 + 12 \cdot 5 = \underline{5} \cdot 13 - 2 \cdot \underline{32}$

El que acompaña al de la x.

$1 = (13 \cdot \underbrace{5) \bmod 5}_{0} - (2 \cdot 32) \bmod 5$

$1 = \underbrace{-2 \cdot 32 \bmod 5}_{\text{Despejamos el 32}}$ $\quad 32^{-1} = -2 \bmod 5 \Rightarrow \underline{x = 3 \bmod 5}$

ÍNDICE

BLOQUE 1: Cálculo de Inversos: resolver ax=1 mod.n, dónde m.c.d(a,n)=1:

1.1 Aplicando el teorema de Fermat:

1. **Resolver: 35x = 1 mod.3**

1.2 Aplicando el teorema de Euler:

2. **Resolver: 17x = 1 mod.12**

1.3 Aplicando el método de Euclides modificado:

<u>Repaso del algoritmo de Euclides para el cálculo del m.c.d. de dos números:</u>

Ejemplo: Cálculo del m.c.d(1547,560)

	2	1	3	4	1	3
1547	560	427	133	28	21	7
427	133	28	21	**7**	**0**	

1547 = 2 * 560 + 427

560 = 1 * 427 + 133

427 = 3 * 133 + 28

133 = 4 * 28 + 21

28 = 1 * 21 + 7

entonces 7 (último resto no nulo) es el m.c.d. de 1547 y 560.

En general, si m.c.d(n,a)=1 entonces:

	c_1	c_2				c_n	c_{n+1}
n	a	r_1	r_2	...	...	r_{n-1}	**1**
r_1	r_2	r_3	...	...	**1**	**0**	

$15x \equiv 6 \bmod 9 \rightarrow 15x + 9y = 6$

$\downarrow$ Simp.

$5x + 3y = 2 \qquad 5x \equiv 2 \bmod 3$

Euclides con mcd 1

3 soluciones $\rightarrow$ $\text{mcd}(15, 9) = 3$

$$\begin{array}{r|l} 15 & 3 \\ 5 & 5 \\ 1 & \end{array} \qquad \begin{array}{r|l} 9 & 3 \\ 3 & 3 \\ 1 & \end{array}$$

$x = \frac{6}{3} y + j\frac{9}{3} \bmod 9 = 2y + j\,3 \bmod 9$

Si mcd 1 es hallar el inverso sino.

$5 = 3 \cdot 1 + 2 \qquad 1 = 3 - 5 + 3 = 2 \cdot 3 - 1 \cdot 5$

$3 = 2 \cdot 1 + 1 \qquad 1 = 3 - 2$

$2 = 1 \cdot 2 + 0$

$x = 5^{-1} \cdot 2 \bmod 3$ ~ Poner resultado en func de la simp. y hallar para el e mod las 3 sol. (+3) (ojo mod 9)

$x = -2 \bmod 3$

$\boxed{x = 1 \bmod 9}$ ~ Sol correcta

4, 7

1.1 Aplicando el teorema de Fermat:

1. **Resolver: 35x = 1 mod.3**

1.2 Aplicando el teorema de Euler:

2. **Resolver: 17x = 1 mod.12**

70 mod 3
10 m
1 mod 3

1.) $\text{mcd}(35, 3) = 1$ Coprimos

$$\begin{array}{r|l} 35 & 5 \\ 7 & 7 \\ 1 & \end{array} \qquad \begin{array}{r|l} 3 & 3 \\ 1 & \end{array}$$

3 primo

$x = 35^{-1} \bmod 3$

$x = 35^{3-2} \bmod 3 = 2^1 \bmod 3$

$-3 \cdot 11$, 2

$$\boxed{x = 2 \bmod 3}$$

2.) $\text{mcd}(17, 12) = 1$

$$\begin{array}{r|l} 17 & 17 \\ 1 & \end{array} \qquad \begin{array}{r|l} 12 & 2 \\ 6 & 2 \\ 3 & 3 \\ 1 & \end{array}$$

12 no primo

$x = 17^{-1} \bmod 12 \qquad \phi(12) = \phi(2^2 \cdot 3) = 2^1 \cdot 1 \cdot 2 = 4$

$x = 17^{4-1} \bmod 12 = 5^3 \bmod 12 = 5 \cdot 5^2 \bmod 12 = 5 \bmod 12$

-12, 5 ; 25, $-2 \cdot 12$, 1

$$\boxed{x = 5 \bmod 12}$$

De donde se obtiene que:

$n = c_1 a + r_1$

$a = c_2 r_1 + r_2$

$r_1 = c_3 r_2 + r_3$

...

...

$r_{n-2} = c_n r_{n-1} + 1$

$r_{n-1} = c_{n+1} + 0$

despejando y sustituyendo en cascada los sucesivos restos se obtiene una expresión del tipo:

$1 = k_1 a + k_2 n$

que reduciendo módulo n se queda en:

$1 = k_1 a \text{ mod.} n$

por tanto $k_1 = a^{-1} \text{ mod.} n$

Ejercicios:

3. **Resolver: 32x = 1 mod.5**

BLOQUE 2: Resolución de ecuaciones del tipo ax=b mod.n, dónde m.c.d(a,n)=1

2.1 Aplicando el teorema de Euler:

4. **Resolver 3x = 3 mod.14**

2.2 Aplicando el método de Euclides modificado:

5. **Resolver 19x = 4 mod.49**

Ejercicios: Euclides

3. Resolver: 32x = 1 mod.5

$mcd(32,5)=1$ ✓

$x = 32^{-1} \bmod 5$

$32 = 5\cdot 6 + 2$
$5 = 2\cdot 2 + 1$
$2 = 1\cdot 2 + 0$

$1 = 5 - 2(32 - 5\cdot 6) = 5\cdot 6 - 2\cdot 32$
$1 = 5 - 2\cdot 2$

$1 = \underbrace{(5\cdot 6) \bmod 5}_{0} - (2\cdot 32) \bmod 5 = -2\cdot 32 \bmod 5$

$32^{-1} = -2 \bmod 5$ $\boxed{x = -2 \bmod 5}$

2.1 Aplicando el teorema de Euler:

4. Resolver 3x = 3 mod.14

2.2 Aplicando el método de Euclides modificado:

5. Resolver 19x = 4 mod.49

4) $3x = 3 \bmod 14 ;\ x = 3\cdot 3^{-1} \bmod 14$

$mcd(3,14)=1$ ✓ $\}$ $3^{-1} = 3^{\phi(14)-1} \bmod 14 = 3^{6-1} \bmod 14 = -1\cdot 9 \bmod 14 = 5 \bmod 14$

$3^3\cdot 3^2 \cdot 9$ $\quad 27-14=13-14=-1$ $\quad -9+14=5$

$\begin{array}{c|c} 3 & 3 \\ 1 & 1 \end{array}$ $\quad \begin{array}{c|c} 14 & 2 \\ 7 & 7 \\ 1 & 1 \end{array}$ $\quad \phi(14) = 1\cdot 6 = 6$

$\boxed{x = 3\cdot 5 \bmod 14 = 1 \bmod 14}$ $\quad 3\cdot 1 \bmod 14 = 3 \bmod 14$

5) $19x = 4 \bmod 49 \ ;\ x = 19^{-1}\cdot 4 \bmod 49$

$49 = 19\cdot 2 + 11$
$19 = 11\cdot 1 + 8$
$11 = 8\cdot 1 + 3$
$8 = 3\cdot 2 + 2$
$3 = 2\cdot 1 + 1$
$2 = 1\cdot 2 + 0$

$1 = 7(49 - 2\cdot 19) - 4\cdot 19 = 7\cdot 49 - 18\cdot 19$
$1 = 11\cdot 3 - 4\cdot(19 - 11) = 7\cdot 11 - 4\cdot 19$
$1 = 3\cdot(11-8) - 8 = 11\cdot 3 - 4\cdot 8$
$1 = 3 - 1(8 - 2\cdot 3) = 3\cdot 3 - 8$
$1 = 3 - 1\cdot 2$

$mcd(19,49)=1$ Coprimos, 1 solución

$1 = (-18\cdot 19) \bmod 49 + (5\cdot 49) \bmod 49$

$1 = -18\cdot 19 \bmod 49;\ 19^{-1} = -18 \bmod 49$

$x = 4\cdot \underbrace{(-18)}_{-72} \bmod 49 = 26 \bmod 49$ $\quad \boxed{x = 26 \bmod 49}$

Compr. $19\cdot 26 = 494 - 10\cdot 49 = \underline{4}$

BLOQUE 3: Resolución de ecuaciones del tipo ax=b mod.n, dónde m.c.d(a,n)=m≠1

Sólo en el caso de que b = cm (c entero) la ecuación tiene solución. Esta solución/-es están en el conjunto {1, 2, 3,... n-1} y viene dada por la expresión:

x=(b/m)y + k(n/m) mod.n k=0,1,...m-1,

Dónde y es la solución de: (a/m)y mod.(n/m)=1.

3.1 Aplicando el teorema de Euler

6. **Resolver 15x = 6 mod. 9**

BLOQUE 4: Misceláneos:

7. **Resolver: 37x = 1 mód.10**

8. **Resolver 3x = 5 mód.8**

9. **Resolver 5x = 10 mod. 15**

10. **Resolver 63x = 2 mod. 110**

11. **Demuestre que:**

Dados M y n tales m.c.d(M,n) =1, y

Dados e,d Є Z-{0} tales que e*d=1 mod. Φ(n), entonces:

M^{e*d} mod. n =M

Añadiendo exponencial en ambos lados:

$M^{e*d} = M^{1} \bmod \underbrace{\varnothing(n)}_{¿?}$

12. **Establezca y razone si son verdaderas o falsas las siguientes igualdades:**

a) $16^{16} + 16^{17}$ mod17 = 1 mod17

b) $16^{17} * 16^{16}$ mod17 ≡ -1 mod17

$\varnothing(14) = 1 \cdot 6 = 6$
$1 \cdot 7$

$1 = 15 \bmod 14$

$15 = 1 \bmod 14$

$\varnothing(n)$

$1 = 15 \bmod 6$

$1 = 3 \bmod 6$

13. **Demuestre que:**

Si a y n son dos enteros tales que, m.c.d. (a,n) = 1, entonces:

$a^x = a^y$ mod. n ⇨ x = y mod. Φ(n).

$\log_a a^x = \log_a a^y \bmod n$

$x = y \bmod n$

3.1 Aplicando el teorema de Euler

6. Resolver 15x = 6 mod. 9

$x = 6 \cdot 15^{-1} \text{ mod. } 9$ $\quad x = 2 \cdot 5^{-1} \text{ mod. } 3$

$\text{mcd}(15,9) = 3 \neq 1$ $\quad \text{mcd}(5,3) = 1 \checkmark \quad \phi(3) = 2$

$15 | 3, \; 5 | 5, \; 1$ $\quad 9 | 3, \; 3 | 3, \; 1$

$1 = 5^{\phi(3)} \text{ mod. } 3$ $\quad 5^{-1} = 5 \text{ mod } 3 = 2 \text{ mod } 3$

$5^{-1} = 5^{\phi(3)-1} \text{ mod. } 3$ $\quad x = 2 \cdot 2 \text{ mod } 3 = 1 \text{ mod } 3$

$\text{mcd} = 3 \neq 1$ 3 Soluciones

$\boxed{x = 1 \text{ mod } 9 \qquad x = 4 \text{ mod } 9 \qquad x = 7 \text{ mod } 9}$

7. Resolver: 37x = 1 mód.10

$\text{mcd}(37,10) = 1$ $\quad x = 37^{-1} \text{ mod } 10$ $\quad \phi(10) = \phi(2)\phi(5) = 1 \cdot 4 = 4$

$10 | 2, \; 5 | 5, \; 1$ $\quad 37 | 37, \; 1$

10 no primo

$37^{-1} = 37^{\phi(10)-1} \text{ mod. } 10 = (-3)^3 \text{ mod } 10 = 3 \text{ mod } 10$

$-27+30$

Solución unica

$\boxed{x = 3 \text{ mod } 10}$ $\quad 3 \cdot 37 = 111 - 10 \cdot 11 = 1$ Comprobado

8. Resolver 3x = 5 mód.8

$\text{mcd}(3,8) = 1$ Solución única $\quad x = 3^{-1} 5 \text{ mod. } 8$ $\quad \phi(8) = \phi(2^3) = 4 \cdot 1 = 4$

2^2

$3 | 3, \; 1$ $\quad 8 | 2, \; 4 | 2, \; 2 | 2, \; 1$

$3^{-1} = 3^{\phi(8)-1} \text{ mod } 8 = 3^2 \cdot 3 \text{ mod } 8 = 3 \text{ mod. } 8$

$9 \cdot 8 = 1$

8 no primo

Compro.

$x = 3 \cdot 5 \text{ mod. } 8 = \boxed{7 \text{ mod } 8 = x}$ $\quad 21 \equiv 5 \text{ mod } 8$

9. Resolver 5x = 10 mod. 15

Se puede simplificar si en todo esta en mcd

$\frac{5}{5} = 1 \quad \frac{10}{5} = 2 \quad \frac{15}{5} = 3$

$\text{mcd}(5,15) = 5$ $\quad x = 2 \text{ mod } 3$

5 soluciones

$\boxed{x = 2 \text{ mod } 15 / x = 5 \text{ mod } 15 / x = 8 \text{ mod } 15 / x = 11 \text{ mod } 15 \quad x = 14 \text{ mod } 15}$

$= \text{mcd}(a,n)$

$m | b$

$5 | 10$

5 soluciones

$\overset{a}{5x} + \overset{b}{15y} = \overset{n}{10}$

$1 \cdot x + 3y = 2$

$\underbrace{1(-1) + 3(1)}_{\text{Los que le ajustan}} = 2$

$1(x+1) + 3(y-1) = 0;$

$1(x+1) = 3(1-y)$

$1k = -y+1, \; y = 1-1k$

$3k = x+1; \; x = 3k-1$ ← la que me interesa

$x = -1 = 14 \quad x = 5 \quad x = 11$

$x = 2 \quad x = 8$

10. Resolver 63x = 2 mod. 110

$mcd(63,110)=1$ Solución unica

$$\begin{array}{r|l} 110 & 2 \\ 55 & 5 \\ 11 & 11 \\ 1 & 1 \end{array} \qquad \begin{array}{r|l} 63 & 3 \\ 21 & 3 \\ 7 & 7 \\ 1 & 1 \end{array}$$

110 no primo

$x = 2 \cdot 63^{-1} \bmod 110$ $\quad \phi(110) = \phi(2)\,\phi(5)\,\phi(11) = 1 \cdot 4 \cdot 10 = 40$

$63^{-1} = 63^{39} \bmod 110 = \underbrace{(63^3)^{13}}_{(17)^{13}} \bmod 110 = \underbrace{(17^4)^3}_{(31)^3 = 91 = -19} \cdot 17 \bmod 110 =$

$63^{-1} = 17 \cdot (-19) \bmod 110 = 7 \bmod 110$

$\boxed{x = 2 \cdot 7 \bmod 110 = 14 \bmod 110}$

12. Establezca y razone si son verdaderas o falsas las siguientes igualdades:

a) $16^{16} + 16^{17} \bmod 17 = 1 \bmod 17$ Falsa

b) $16^{17} * 16^{16} \bmod 17 = -1 \bmod 17$ Verdadera

a) $(\underbrace{16^{16}}_{\frac{-17}{(-1)^{16}}} + \underbrace{16^{17}}_{\frac{-17}{(-1)^{17}}}) \bmod 17 = (\cancel{1+(-1)}) \bmod 17 = 0 \bmod 17$ Falsa

b) $(\underbrace{16^{17}}_{\frac{-17}{(-1)^{17}}} \cdot \underbrace{16^{16}}_{\frac{-17}{(-1)^{16}}}) \bmod 17 = (-1 \cdot 1) \bmod 17 = -1 \bmod 17$ Verdadera

$2^{68} : 19$ $\quad \phi(19) = 18$

Euler $\quad 1 = 2^{18} \bmod 19$ $\qquad 1^3 \cdot 2^{14} = (2^{18})^3 \cdot 2^{14} \bmod 19$

$2^{14} = 2^{68} \bmod 19 = (2^7)^2 = -5^2 = 25 = 6$

$14^2 = -5^2$ $\qquad \frac{25 - 19}{6}$

$6 = 2^{68} \bmod 19$

→ Resto $2^{68} : 19$

14. Demuestre que:

Dados a, b, c, n Є Z-{0} tales que m.c.d(a,n)=d, si ab ≡ ac mod.n ⇨ b ≡ c mod. n/d.

$ab - ac = n \cdot k$

$\frac{a}{d}b - \frac{a}{d}c = \frac{n}{d}k \Rightarrow \cancel{\frac{a}{d}}b \equiv \cancel{\frac{a}{d}}c \bmod \frac{n}{d}$

$* \; b \equiv c \bmod n/d$

15. Demuestre que:

Demuestre que el sistema de ecuaciones siguiente no tiene solución:

$$\begin{cases} x=2 \text{ mod.}6 \\ x=3 \text{ mod.}9 \end{cases}$$

$x-2 = 6 \cdot k \;/\; k \in \mathbb{Z}$

$x-3 = 9 \cdot k'$

$/ \; 1 = -3(k \cdot k'); \; \boxed{k = -1/3 \notin \mathbb{Z} \text{ No es posible}}$

$(k \cdot k') \in \mathbb{Z}$