Universidad Carlos III de Madrid
Carlos III de Madrid
COSEC LAB· Dpto. Informática

Universidad Carlos III de Madrid

Problemas fundamentos matemáticos

SOLUCIONES

CSI
Curso 2016/2017

Almudena Alcaide Raya

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

Solución

a=35, n=3 primo, m.c.d.(35,3)=1, por Fermat: x= 35n-2 mod.3 ⇨

x=353-2 mod.3 ⇨ x=35 mod.3 ⇨ x= 2 mod.3

1.2 Aplicando el teorema de Euler:

2. Resolver: 17x = 1 mod.12

Solución

a=17, n=12 (no primo), m.c.d.(17,12)=1, por Euler: $x = 17^{\Phi(12)-1}$ mod.12

Aquí, $12 = 2^2 * 3$, $\Phi(12) = \Phi(2^2) * \Phi(3) = 2^{2-1} * (2-1) * 2 = 4$

$x = 17^{4-1}$ mod.12 ⇨ $x = 17^3$ mod.12 ⇨ $x = 5^3$ mod.12

⇨ (Por reducción modular) x = 5 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**	

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

Solución

(La solución es inmediata si se realiza una reducción modular de la ecuación, resultando en: 2x mod.5=1).

Para ilustrar el manejo del método de Euclides modificado se elige calcular el inverso aplicando dicho método:

	6	2	2
32	5	2	1
2	1	0	

$a = c_1 n + r_1 \Rightarrow r_1 = a - c_1 n$

$n = c_2 r_1 + r_2 \Rightarrow r_2 = n - c_2 r_1$

$\Rightarrow r_2 = n - c_2 (a - c_1 n) \Rightarrow r_2 = n\ (1+c1c2) - c_2 (a - c_1 n) \Rightarrow$

$r_2 = n\ (1+ c_1\ c_2) - c_2\ a$

entonces: $r_2 = 1= n\ (1+ c_1\ c_2) - c_2\ a \Rightarrow 1= - c_2\ a \text{ mod. } n \Rightarrow$

$1 = -2 * 32 \text{ mod. } 5 \Rightarrow x \equiv -2 \text{ mod.}5 \Rightarrow x = 3 \text{ mod.}5$

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

Solución

a=3, n=14 (no primo), m.c.d.(14,3)=1, por Euler: $a^{-1} = 3^{\Phi(14)-1}$ mod.14

Aquí, 14 = 7*2, $\Phi(14) = \Phi(7) * \Phi(2) = (7\text{-}1) * (2\text{-}1) = 6*1 = 6$

$a^{-1} = 3^{6-1}$ mod.14 $\Rightarrow a^{-1} = 3^5$ mod.14 $\Rightarrow a^{-1}$ = 9*9*3 mod.14= 243 mod.14= 5 mod.12

$\Rightarrow$ (Por reducción modular) a^{-1} = 5 mod.14

x= a^{-1}*b = 5 * 3 mod.14= 1

2.2 Aplicando el método de Euclides modificado:

5. Resolver 19x = 4 mod.49

Solución:

19y = 1 mod.49, dónde x=y*4 mod.49

$n = c * a + r_1$

49 = 19 * 2 + 11

19 = 11 * 1 + 8

11= 8 *1 +3

8 = 3*2 +2

3 = 2*1 +1

----

r_1= n-2a

r_2=a -r_1= a-n +2a= 3a -n

r_3=r1-r_2= n-2a -(3a -n) = -5a +2n

r_4=r_2-2r_3= 3a -n -2(-5a +2n) = 13a -5n

1= r_3 – r_4= -5a +2n - 13a +5n= -18a +7n

1 = -18a mod.49

y = -18 mod.49 = 31 mod.49

x = 4 * y mod.49 = 4*31 mod.49= 26 mod.49

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

Solución: La ecuación es equivalente a ésta otra: 6x=6 (mod. 9)

a= 6, n=9, m.c.d.(6,9)= *m = 3*

b = 6 = 2 * *m*

Se calcula y:

2y (mod. 3) = 1

por Euler y =2^1 (mod. 3); y = 2

Por lo tanto:

x = (6/3)*2 + (9/3)k ;

x = 4 + 3k mod.9, para k= {0,1,2}

BLOQUE 4: Misceláneos:

7. Resolver: 37x = 1 mód.10

Solución

a=37, n=10, m.c.d.(37,10)=1, por Euler: x = $37^{\Phi(10)-1}$ mód.10

Aquí, 10 = 2 * 5, Φ(10) = Φ(2) * Φ(5) = 1 * 4 = 4

x = 37^{4-1} mód.10 ⇨ x = 37^3 mód.10 ⇨ x = 7^3 mód.10 ⇨ x = 63 mód.10 ⇨

x = 3 mód.10

8. Resolver 3x = 5 mód.8

Solución

Transformamos a 3y (mód.8) = 1 dónde x=y*5 mód.8.

Para resolverlo aplicamos el teorema de Euler x = $a^{\phi(n)-1}$ mód.n

Por ϕ(n) = n^{k-1} (n-1) se obtiene que ϕ(8) = 4,

y = $3^{\phi(8)-1}$ mód.8 = 3^3 (mód.8) ⇨ y = 3 mód.8

Despejamos en x = by (mód.n), y resolvemos:

x = 15 (mód.8) ⇨ x = 7 mód.n

9. Resolver 5x = 10 mod. 15

Solución

m.c.d.(15,5)= **5 = m**

y (mód.3) = 1

por Euler y =1 (mód.3); y = 1

Por lo tanto:

x = (10/5).1 + (15/5).k ;

x = 2 * 1 + 3.k , para k= {0,1,2,3,4}

10. Resolver 63x = 2 mod. 110

	1	1	2	1	15
110	63	47	16	15	**<u>1</u>**
47	16	15	**<u>1</u>**	**<u>0</u>**	

$n = c_1 a + r_1 \Rightarrow r_1 = n - c_1 a$

$a = c_2 r_1 + r_2 \Rightarrow r_2 = a - c_2 r_1$

$r_1 = c_3 r_2 + r_3 \Rightarrow r_3 = r_1 - c_3 r_2$

$r_2 = c_4 r_3 + r_4 \Rightarrow r_4 = r_2 - c_4 r_3 = \underline{\mathbf{1}}$

$r_3 = c_5 r_4 + r_5 \Rightarrow r_5 = \underline{\mathbf{0}}, c_5 = \underline{\mathbf{1}}$

$\underline{110} = 1 \cdot \underline{63} + 47 \Rightarrow \mathbf{47} = \underline{110} - 1 \cdot \underline{63}$

$\underline{63} = 1 \cdot 47 + 16 \Rightarrow \mathbf{16} = \underline{63} - 1 \cdot 47$

$47 = 2 \cdot 16 + 15 \Rightarrow \mathbf{15} = 47 - 2 \cdot 16$

$16 = 1 \cdot 15 + 1 \Rightarrow \underline{\mathbf{1}} = 16 - 1 \cdot 15$

$15 = 15 \cdot 1 + \underline{\mathbf{0}}$

$\underline{\mathbf{1}} = 16 - 1 \cdot 15 =$

$= (\underline{63} - 1 \cdot 47) - 1 \cdot (47 - 2 \cdot 16) =$

$= (\underline{63} - 1 \cdot (\underline{110} - 1 \cdot \underline{63})) - 1 \cdot (\underline{110} - 1 \cdot \underline{63} - 2 \cdot (\underline{63} - 1 \cdot 47)) =$

$= (\underline{63} - 1 \cdot (\underline{110} - 1 \cdot \underline{63})) - 1 \cdot (\underline{110} - 1 \cdot \underline{63} - 2 \cdot (\underline{63} - 1 \cdot (\underline{110} - 1 \cdot \underline{63}))) =$

$= -4 \cdot \underline{110} + 7 \cdot \underline{63}$

$1 = -4 \cdot \underline{110} + 7 \cdot \underline{63}$ mod.110 = $7 \cdot 63$ mod.110

63^{-1} mod.110 = 7

X = 7 · 2 mod 110 = 14

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. $\Phi(n)$, entonces:

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

Solución: (Esta es la demostración del algoritmo RSA)

e*d = 1 mod $\Phi(n)$ → e*d = k*$\Phi(n)$ + 1

m.c.d(M,n)=1 ⇨(por T^{ma}. Euler) $M^{\Phi(n)}$= 1 mod n ⇨ $M^{k*\Phi(n)}$ = 1 mod n

Entonces:

M^{e*d} mod n = $M^{(k*\Phi(n)+1)}$mod n = $M^{k*\Phi(n)} \cdot$ M mod n = M mod 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

Solución:

Se aplica el teorema de Fermat: a^{16} mod17 = 1 para m.c.d(a,17)=1

a) (falso = 0)

b) Verdadero (la igualdad no hubiera sido verdadera)

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. $\Phi(n)$.

Solución:

Partimos:

$a^x = a^y$ mod. n ;

a^{x-y} = 1 mod. n ;

$a^{\Phi(n)}$ = 1 mod. n; Teorema de Euler

Entonces: x-y = k * $\Phi(n)$; para k entero.

Entonces: x = y mod. $\Phi(n)$

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.

Solución:

ab ≡ ac mod..n ⇨ existe k entero tal que ab – ac = kn (1)

m.c.d (a,n)=d ⇨ existe k_a entero tal que k_a = a/d

m.c.d (a,n)=d ⇨ existe k_n entero tal que k_n = n/d y además m.c.d(k_a, k_n)=1

Dividimos (1) entre d:

a/d(b – c) = k n/d ⇨ k_a (b – c) = k k_n ⇨ k_a divide a k ⇨

(b – c) = k/ k_a n/d ⇨ b ≡ c mod. n/d

15. Demuestre que:

Demuestre que el sistema de ecuaciones siguiente no tiene solución:

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

Solución:

x=2 mod.6 ⇨ existe k entero tal que x=6k + 2

6k + 2 = 3 mod.9 ⇨ 6k = 1 mod.9, m.c.d(6,9)=3≠1 ⇨ No existe solución a esta ecuación ¡!