Universidad Carlos III de Madrid

CURSO CRIPTOGRAFÍA Y SEGURIDAD INFORMÁTICA

Ana I. González-Tablas Ferreres
José María de Fuentes García-Romero de Tejada
Lorena González Manzano
Pablo Martín González
UC3M | GRUPO COMPUTER SECURITY LAB (COSEC)

"Fundamentos matemáticos"

Ejercicios propuestos

Ejercicio 1 :

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

a) Aplicando el teorema de Fermat. Resolver: 37x = 1 mod.5

b) Aplicando el teorema de Euler. Resolver: 7x = 1 mod.12

c) Aplicando el método de Euclides modificado. Resolver: 32x = 1 mod.5

Solución:

a)

a=37, n=5 primo, m.c.d.(37,5)=1, por Fermat: $x = 37^{n-2}$ mod.5 ⇨

$x=37^{5-2}$ mod.5 ⇨ x=3 mod.5

b)

a=7, n=12 (no primo), m.c.d.(7,12)=1, por Euler: $x = 7^{\Phi(12)-1}$ mod.12

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

$x = 7^{4-1}$ mod.12 ⇨ $x = 7^3$ mod.12 ⇨ x = 7 mod.12

c)

(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: $r_2 = 1 = n\ (1+ c_1\ c_2) - c_2\ a \Rightarrow 1 = - c_2\ a \bmod.\ n \Rightarrow$

$1 = -2 * 32 \bmod.\ 5 \Rightarrow x \equiv -2 \bmod.5 \Rightarrow x = 3 \bmod.5$

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

a) Aplicando el teorema de Euler. Resolver 3x = 3 mod.14

b) Aplicando el método de Euclides modificado. Resolver 19x = 4 mod.49

Solución:

a)

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, $\Phi(14) = \Phi(7) * \Phi(2) = (7-1) * (2-1) = 6*1 = 6$

$a^{-1} = 3^{6-1}$ 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

b)

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

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

a) Aplicando el teorema de Euler. Resolver 15x = 6 mod. 9

Solución:

a)

L a 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 =21 (mod. 3); y = 2

Por lo tanto:

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

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

Ejercicio 4:
Ejercicios misceláneos de aritmética modular

a) Sin indicar el método.
   i) Resolver: $2x = 1$ mód.4
   ii) Resolver: $37x = 1$ mód.10
   iii) Resolver $3x = 5$ mód.8
   iv) Resolver $5x = 10$ mod. 15
   v) Resolver $63x = 2$ mod. 110
b) Demostración de propiedades
   i) Demuestre que:

      Dados M y n tales m.c.d(M,n) =1, y
      Dados e,d ∈ Z-{0} tales que e*d=1 mod. $\Phi(n)$, entonces:
      M^{e*d} mod. n =M

   ii) Establezca y razone si son verdaderas o falsas las siguientes igualdades:

      ii.a) $16^{16} + 16^{17} \text{ mod} 17 = 1 \text{ mod} 17$
      ii.b) $16^{17} * 16^{16} \text{ mod} 17 \equiv -1 \text{ mod} 17$

   iii) 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. $\Phi(n)$.

   iv) Demuestre que:

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

   v) 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:

a)

i) Resolver: 2x = 1 mód.4

a=2, n=4, m.c.d.(2,4)≠1, por lo que no existe solución.

ii) Resolver: 37x = 1 mód.10

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

Aquí, 10 = 2 * 5, $\Phi(10) = \Phi(2) * \Phi(5) = 1 * 4 = 4$

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

x = 3 mód.10

iii) Resolver 3x = 5 mód.8

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 $\phi(n) = n^{k-1}(n-1)$ se obtiene que $\phi(8) = 4$,

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

iv) Resolver 5x = 10 mod. 15

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}

v) Resolver 63x = 2 mod. 110

	1	1	2	1	15
110	63	47	16	15	**1**
47	16	15	**1**	**0**	

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

63^{-1} mod.110 = 7

X = $7 \cdot 2$ mod 110 = 14

b)

i)

(Ésta es la demostración del algoritmo RSA)

$e*d = 1 \bmod \Phi(n) \rightarrow e*d = k*\Phi(n) + 1$

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

Entonces:

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

ii)

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

ii.a) (falso = 0)

ii.b) Verdadero (la igualdad no hubiera sido verdadera)

iii)

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. $\Phi(n)$

iv)

$ab \equiv ac$ 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 ⇨

$(b - c) = k/ k_a\, n/d$ ⇨ $b \equiv c$ mod. n/d v)

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

$6k + 2 = 3$ mod.9 ⇨ $6k = 1$ mod.9, m.c.d(6,9)=$3\neq1$ ⇨ No existe solución a esta ecuación