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

**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

**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

**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) $16^{16} + 16^{17} \mathrm{mod} 17 = 1 \mathrm{mod} 17$

ii.b) $16^{17} * 16^{16} \mathrm{mod} 17 \equiv -1 \mathrm{mod} 17$

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 ≡ ac mod.n ⇨ b ≡ c mod. n/d.

v) Demuestre que:

Demuestre que el sistema de ecuaciones siguiente no tiene solución:

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