Ana I. González-Tablas Ferreres
José María de Fuentes García-Romero de Tejada
Lorena González Manzano
Sergio Pastrana Portillo
UC3M | COMPUTER SECURITY LAB (COSEC) GROUP

Mathematical background

Proposed exercises

Exercise 1 :

Computing inverses. Solve ax=1 mod.n, when g.c.d(a,n)=1

a) Applying Fermat's theorem. Solve: 37x = 1 mod.5

b) Applying Euler's theorem. Solve: 7x = 1 mod.12

c) Applying modified Euclid's algorithm. Solve: 32x = 1 mod.5

Key:

a)

a=37, n=5 prime, g.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 (not prime), g.c.d.(7,12)=1, by Euler: x = $7^{\Phi(12)-1}$ mod.12

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

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

c)

(The key is straightforward if the equation is reduced, leading to 2x mod.5=1).

In order to show how Euclid's algorithm should be applied to compute inverses, the process is illustrated below:

	6	2	2
32	5	2	1
2	1	0	

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

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

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

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

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

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

Exercise 2:

Solve ax=b mod.n equations, when g.c.d(a,n)=1

a) Applying Euler's theorem. Solve 3x = 3 mod.14

b) Applying modified Euclid's algorithm. Solve 19x = 4 mod.49

Key:

a)

a=3, n=14 (not prime), g.c.d.(14,3)=1, by Euler: $a^{-1} = 3^{\Phi(14)-1}$ mod.14

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

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

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

$x = a^{-1} \cdot b = 5 \cdot 3$ mod.14= 1

b)

19y = 1 mod.49, where $x = y \cdot 4$ mod.49

$n = c \cdot a + r_1$

$49 = 19 \cdot 2 + 11$

$19 = 11 \cdot 1 + 8$

$11 = 8 \cdot 1 + 3$

$8 = 3 \cdot 2 + 2$

$3 = 2 \cdot 1 + 1$

$r_1 = n - 2a$

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

Exercise 3:
Solve ax=b mod.n equations, when g.c.d(a,n)=m≠1

a) Applying Euler's theorem. Solve 15x = 6 mod. 9

Key:

a)

The equation is equivalent to: 6x=6 (mod. 9)

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

b = 6 = 2 · m

Computing y:

2y (mod. 3) = 1

By Euler   y =21 (mod. 3); y = 2

Therefore:

x = (6/3)·2 + (9/3) · k ;

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

Exercise 4:
Modular arithmetic. Miscellaneous exercises

a) Using your preferred method.
   i) Solve: 2x = 1 mod.4
   ii) Solve: 37x = 1 mod.10
   iii) Solve 3x = 5 mod.8

iv) Solve $5x = 10 \text{ mod. } 15$

v) Solve $63x = 2 \text{ mod. } 110$

b) Mathematical proofs on properties:

i) Proof that:

Given M, n such that g.c.d(M,n) =1, and
Given e,d Є Z-{0} such that $e \cdot d=1 \text{ mod. } \Phi(n)$, then the following expression holds:
$M^{e \cdot d} \text{ mod. } n = M$

ii) Justify whether these statements are true or false:

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

ii.b) $16^{17} \cdot 16^{16} \bmod 17 \equiv -1 \bmod 17$

iii) Proof that:

Given a, n integers such that g.c.d. (a,n) = 1, then:
$a^x = a^y \text{ mod. } n \Rightarrow x = y \text{ mod. } \Phi(n)$.

iv) Proof that:

Given a, b, c, n Є Z-{0} such that g.c.d(a,n)=d, if $ab \equiv ac \text{ mod.} n \Rightarrow b \equiv c \text{ mod. } n/d$.

v) Proof that the following system has no solution:

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

Key:

a)

i) Solve: $2x = 1 \text{ mod.} 4$

a=2, n=4, g.c.d.(2,4)≠1, thus, there is no key.

ii) Solve: $37x = 1 \text{ mod.} 10$

a=37, n=10, g.c.d.(37,10)=1, by Euler: $x = 37^{\Phi(10)-1}$ mod.10

Then, $10 = 2 \cdot 5$, $\Phi(10) = \Phi(2) \cdot \Phi(5) = 1 \cdot 4 = 4$

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

x = 3 mod.10

iii) Solve 3x = 5 mod.8

We transform it into 3y (mod.8) = 1 where $x=y\cdot 5$ mod.8.

By Euler's theorem $x = a^{\phi(n)-1}$ mod.n

Since $\phi(n) = n^{k-1}(n-1)$ we get $\phi(8) = 4$,

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

Isolating x = by (mod.n), we finally solve:

x = 15 (mod.8) ⇨ x = 7 mod.n

iv) Solve 5x = 10 mod. 15

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

y (mod.3) = 1

by Euler   y =1 (mod.3); y = 1

Then:

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

$x = 2 \cdot 1 + 3.k$,   for k= {0,1,2,3,4}

v) Solve 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>	

$$\left.\begin{aligned}
&n = c_1a + r_1 \Rightarrow r_1 = n - c_1a\\
&a = c_2r_1 + r_2 \Rightarrow r_2 = a - c_2r_1\\
&r_1 = c_3r_2 + r_3 \Rightarrow r_3 = r_1 - c_3r_2\\
&r_2 = c_4r_3 + r_4 \Rightarrow r_4 = r_2 - c_4r_3 = \underline{\mathbf{1}}\\
&r_3 = c_5r_4 + r_5 \Rightarrow r_5 = \underline{\mathbf{0}},\ c_5 = \underline{\mathbf{1}}
\end{aligned}\right\}\longrightarrow$$

$$\left.\begin{aligned}
&\underline{110} = 1\cdot\underline{63} + 47 \Rightarrow \mathbf{47} = \underline{110} - 1\cdot\underline{63}\\
&\underline{63} = 1\cdot 47 + 16 \Rightarrow \mathbf{16} = \underline{63} - 1\cdot 47\\
&47 = 2\cdot 16 + 15 \Rightarrow \mathbf{15} = 47 - 2\cdot 16\\
&16 = 1\cdot 15 + 1 \Rightarrow \underline{\mathbf{1}} = 16 - 1\cdot 15\\
&15 = 15\cdot 1 + \underline{\mathbf{0}}
\end{aligned}\right\}\longrightarrow$$

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

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

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

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

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

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

$63^{-1} \bmod .110 = 7$

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

b)

i)

(This is the proof of RSA)

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

g.c.d(M,n)=1 $\Rightarrow$(by Euler's theorem) $M^{\Phi(n)} = 1 \bmod n \Rightarrow M^{k\cdot\Phi(n)} = 1 \bmod n$

Then:

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

ii)

Applying Fermat's theorem: $a^{16} \mod 17 = 1$ if $g.c.d(a,17)=1$

ii.a) (False = 0)

ii.b) True (it wouldn't be if it were an equality)

iii)

We start by:

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

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

$a^{\Phi(n)} = 1 \mod. n$; By Euler's theorem

Then: $x-y = k \cdot \Phi(n)$; for any integer k.

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

iv)

$ab \equiv ac \mod.. n$ ⇨ there is an integer k such that $ab - ac = kn$ (1)

$g.c.d(a,n)=d$ ⇨ there is an integer k_a such that $k_a = a/d$

$g.c.d(a,n)=d$ ⇨ there is an integer k_n such that $k_n = n/d$ and that $g.c.d(k_a, k_n)=1$

Dividing (1) by d:

$a/d(b - c) = k\, n/d$ ⇨ $k_a (b - c) = k\, k_n$ ⇨ k_a is a divisor of k ⇨

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

v)

$x=2 \mod. 6$ ⇨ there is an integer k such that $x=6k + 2$

$6k + 2 = 3 \mod. 9$ ⇨ $6k = 1 \mod. 9$, $g.c.d(6,9)=3 \neq 1$ ⇨ There is no key