Examen-1-2016-Solucionesv3buenas.pdf

Examenes

CRIPTOGRAFÍA Y SEGURIDAD INFORMÁTICA
GRADO EN INGENIERÍA INFORMÁTICA
Examen 1 Parcial Evaluación Continua   Leganés/Colmenarejo – Semana 3 – 2016
Apellidos: **Nombre:**
Grupo **Modelo 1**

EJERCICIO 1 (0,2 puntos)

Cálculo de inversos: Aplicando el Teorema de Euler:

A) 7·x mód 22 = 1

SOLUCION:
Como mcd (7, 22) = 1 podemos aplicar el teorema de Euler; y $\Phi(22) = \Phi(2) \cdot \Phi(11)=10$
$x=^{\Phi(n)-1}$ mod 22 = 7^{10-1} mod 22 = 7^9 mod 22 = $7\cdot(7^2)^4$ mod 22 = $7\cdot5^4$ mod 22 = (7·3·3) mód 22 = 19
Solución: x=19

B) 3·x mód. 165 = 1

SOLUCION:
Como mcd (3, 165) = 3 no podemos aplicar el teorema de Euler

EJERCICIO 2 (0,2 puntos)

Cálculo de inversos: Aplicando el método de Euclides modificado:

61·x mod 197 = 1

Sol:

197 = 61 · 3 + 14
61 = 14·4 + 5
14 = 5·2 + 4
5 = 4·1+1

1 = 5 – 4 = 5 – (14 – 5·2) = 3·5 – 14 = 3 · (61 – 14·4) – 14 = 3·61 -13·14 = 3·61 - 13·(197-3·61)=42·61 -13·197
Sol: x = 42

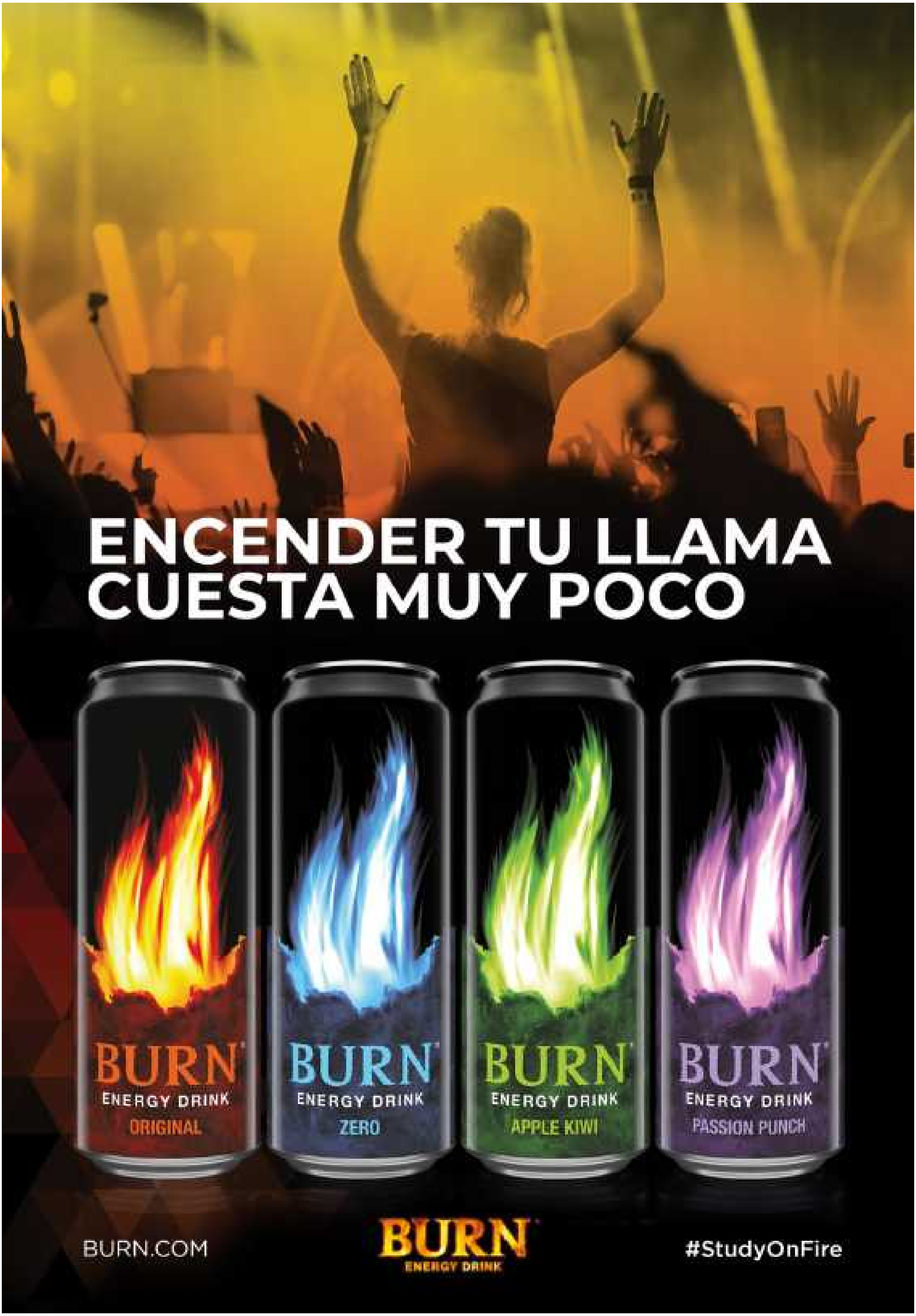
EJERCICIO 3 (0,1 puntos)

Resuelva:

11^{4200} mod 6125 = x

SOLUCION:
$6125= 5^3\cdot 7^2$, luego
$\Phi(6125) = (5^{(3-1)}*(5-1))* (7^{(2-1)}*(7-1)) = (100)*(42) = 4200$
Dado que mcd(11,6125) = 1, por Teorema de Euler, $a^{\Phi(n)}$ mod n = 1

Solución: x=1


ENCENDER TU LLAMA
CUESTA MUY POCO
BURN
ENERGY DRINK
ORIGINAL
BURN
ENERGY DRINK
ZERO
BURN
ENERGY DRINK
APPLE KIWI
BURN
ENERGY DRINK
PASSION PUNCH
BURN.COM
BURN
ENERGY DRINK
#StudyOnFire

CRIPTOGRAFÍA Y SEGURIDAD INFORMÁTICA
GRADO EN INGENIERÍA INFORMÁTICA
Examen 1 Parcial Evaluación Continua Leganés/Colmenarejo – Semana 3 – 2016
Apellidos: **Nombre:**
Grupo **Modelo 1**

EJERCICIO 4 (0,2 puntos)
Resolución de ecuación de congruencia a·x ≡ b mód n

A) 7·x=21 mod 28

SOLUCION:
mcd (7, 28) = 7 y 7 es divisor de 21, por lo que hay 7 soluciones, siendo a=7, b=21, n=28 y m=7:
x_k= (b/m)y+k(n/m) mod n ; k = (0…6)
(a/m)y mod (n/m)=1;

(7/7)y mod (28/7)=1; y mod 4 =1 ; y=1
X_k= 3·1+k·4 mod 28 , luego:
Soluciones:
K=0, x=3
K=1, x=7
K=2, x=11
K=3, x=15
K=4, x=19
K=5, x=23
K=6, x=27

B) 31·x=12 mod79

SOLUCION: mcd (31, 79) = 1, existe solución y es única:
31y mod 79 = 1, aplicando Euclides,

79 = 31·2+17

31= 17 · 1 + 14

17 = 14 ·1 + 3

14 = 3·4 + 2

3=2 + 1

1= 3-2=3-(14-3·4)=5·3-14=5·(17-14)-14=5·17-6·14=5·17-6·(31-17)=11·17-6·31=
11·(79-2·31)-6·31=11·79-28·31,

y=-28 mod 79 = 51

x = 51 ·12 mod 79 = 612 mod 79 = 59

CRIPTOGRAFÍA Y SEGURIDAD INFORMÁTICA
GRADO EN INGENIERÍA INFORMÁTICA
Examen 1 Parcial Evaluación Continua Leganés/Colmenarejo – Semana 3 – 2016
Apellidos: **Nombre:**
Grupo **Modelo 1**

EJERCICIO 5 (0,1 puntos)

Indique si 7 es raíz primitiva del módulo 23.

Solución: Sí lo es. Los divisores de Φ(p-1)= Φ(23)=22 son {1, 2, 11}. Comprobándolo sale que sí lo es.

EJERCICIO 6 (0,2 puntos)

Calcule la operación que sigue con polinomios pertenecientes a CG(2^4) siendo el mod (p(x)), donde p(x) = x^4+x+1.

A) Siendo a(x) =(x^3+x^2), calcule $a(x)^2$ mod p(x)

Solución: $a(x)^2 = x^6+x^4$ en CG(2^4) , y reduciendo,
x^6+x^4 mod $x^4+x+1 = x^3+x^2+x+1$

CRIPTOGRAFÍA Y SEGURIDAD INFORMÁTICA
GRADO EN INGENIERÍA INFORMÁTICA

Examen 1 Parcial Evaluación Continua Leganés/Colmenarejo – Semana 3 – 2016

Apellidos: **Nombre:**

Grupo **Modelo 2**

EJERCICIO 1 (0,2 puntos)

Cálculo de inversos: Aplicando el Teorema de Euler:

A) 9·x mód 41 = 1

SOLUCIÓN:

Como mcd (9, 41) = 1 podemos aplicar el teorema de Euler; y $\Phi(41) = 40$

$x=9^{\Phi(41)-1}$ mod 41 = 9^{39} mod41 = $9\cdot(9^2)^{19}$ mod 41 = $9\cdot(-1)^{19}$ mod 41 = -9 mod 41 = 32

Solución: x=32

B) 7·x mód 72 = 1

SOLUCIÓN:

Como mcd (7, 72) = 1 podemos aplicar el teorema de Euler; si $72=3^2 \cdot 2^3$, $\Phi(72) =(3^{2-1}\cdot(3-1))*(2^{3-1}\cdot(2-1))=6\cdot4=24$

$x=7^{\Phi(72)-1}$ mod 72 = 7^{23} mod 72 = $49 \cdot (7^3)^7$ mod 72 = $49 \cdot 55^7$ mod 72 = $49 \cdot 55$ mod 72 = 31

Solución: x=31

EJERCICIO 2 (0,2 puntos)

Cálculo de inversos: Aplicando el método de Euclides modificado:

23·x mod 47 = 1

Solución:

47=23·2+1

x = -2 = 45 mod 47

CRIPTOGRAFÍA Y SEGURIDAD INFORMÁTICA
GRADO EN INGENIERÍA INFORMÁTICA
Examen 1 Parcial Evaluación Continua Leganés/Colmenarejo – Semana 3 – 2016
Apellidos: **Nombre:**
Grupo **Modelo 2**

EJERCICIO 3 (0,1 puntos)

Razone si existe algún número "s" tal que

$$3^s \text{ mód } 13 = 1$$

En caso de existir, indique cuántos podrían existir. A la vista de lo anterior, ¿es 3 raíz primitiva de 13?

SOLUCIÓN:
Sí, existe seguro pues mcd(3,13)=1, por tanto, como mínimo y por el Tma. Euler, s=Φ(13)=12.
Los números "s" que satisfacen esa condición son divisores de p-1=12, siendo esos divisores {1,2,3,4,6,12}. Por tanto, probamos:
3 mod 13 = 3
9 mod 13 = 9
27 mod 13 = 1 , luego s=3 también cumple la ecuación. Esto implica que 3 no es raíz primitiva de 13.

EJERCICIO 4 (0,2 puntos)

Resolución de ecuación de congruencia a·x ≡ b mód n

A) 19·x=20 mod 37

SOLUCIÓN:
mcd (19, 37) = 1, solución única:

19y mod 37 = 1, resolviendo por Euclides:
37= 19 ·1 + 18
19=18 + 1,
1= 19-18=19-(37-19)=2·19-37 , de lo que y=2
x=20y mod 37 = 40 mod 37 = 3

B) 15·x=12 mod 21

SOLUCIÓN:
mcd (15, 21) = 3 y 3 divide a 12, por lo que hay 3 soluciones, para k=0,1,2 siendo a=15, b=12, n=21 y m=3,
x_k= (b/m)y + k(n/m) mod n ; k = (0,1,2)
(a/m)y mod (n/m)=1;

(15/3)y mod (21/3) = 1; 5y mod 7 = 1; y = 3

X_k = (4·3+k·7) mod 21 = (12 + 7·k) mod 21 , con k=(0,1,2)

Solución: x_k = (12,19,5)

EJERCICIO 5 (0,1 puntos)

¿Cuántos números positivos, menores que 3267, son primos relativos con él?

Sol: $\Phi(3267)= \Phi(11^2 \cdot 3^3) = (11^{2-1} \cdot (11-1)) \cdot (3^{3-1}(3-1)) = (110) \cdot 18 = 1980$

EJERCICIO 6 (0,2 puntos)

Sean los polinomios $a(x)=x^2+1$ y $b(x)= x^2$ pertenecientes a $CG(2^3)$ siendo el mod (p(x)), donde $p(x) = x^3+x+1$. Calcule el polinomio $c(x) = a(x)^2 \cdot b(x)$ mód p(x)

SOLUCIÓN:
$c(x)= (x^4+1) \cdot x^2 = x^6 + x^2 \bmod x^3+x+1 = 1$

CRIPTOGRAFÍA Y SEGURIDAD INFORMÁTICA
GRADO EN INGENIERÍA INFORMÁTICA
Examen 1 Parcial Evaluación Continua Leganés/Colmenarejo – Semana 3 – 2016
Apellidos: **Nombre:**
Grupo **Modelo 3**

EJERCICIO 1 (0,2 puntos)
Cálculo de inversos: Aplicando el Teorema de Euler:

A) 6·x mód 42 = 1

SOLUCIÓN:
No se puede aplicar pues mcd(6,42)=6

B) 3·x mód 77 = 1

SOLUCIÓN:
Como mcd (3, 77) = 1 podemos aplicar el teorema de Euler; si 77=11·7, Φ(77) =10·6 = 60
$x=3^{\Phi(77)-1}$ mod 77 = 3^{59} mod 77 = 27· $(3^4)^{14}$ mod 77 = 27· $(-4)^{14}$ mod 77 = 27· $(16)^7$ mod 77 =27 · 16 · 25^3 mod 77 = 47 · 25^3 mod 77 = 47 · 25 · 9 mod 77 = 26
Solución: x=26

EJERCICIO 2 (0,2 puntos)
Cálculo de inversos: Aplicando el método de Euclides modificado:

26·x mod 113 = 1
Solución:
113 = 26 · 4 + 9
26 = 9 · 2 + 8
9 = 8 + 1

1=9-8=9-(26-9·2)=9·3-26=(113-26·4)·3 -26 = 3·113 -13·26
X= -13 mod 113 = 100

CRIPTOGRAFÍA Y SEGURIDAD INFORMÁTICA
GRADO EN INGENIERÍA INFORMÁTICA
Examen 1 Parcial Evaluación Continua   Leganés/Colmenarejo – Semana 3 – 2016
Apellidos: **Nombre:**
Grupo   **Modelo 3**

EJERCICIO 3 (0,1 puntos)

Calcule

2^{1960} mód 131

Sol:

$\Phi(131)=130$ y $2^{\Phi(131)}$ mód 131 =1 dado que mcd (2,131) =1

2^{1960} mód 131 = $(2^{130})^{15} \cdot 2^{10}$ mód 131 = 1024 mod 131 = 107

EJERCICIO 4 (0,2 puntos)

Resolución de ecuación de congruencia a·x ≡ b mód n

A) 7·x=21 mod 91

SOLUCIÓN:
mcd (7, 91) = 7 y 7 divide a 21, por lo que hay 7 soluciones, para k=0,…6 siendo a=7, b=21, n=91 y m=7,
x_k= (b/m)y + k(n/m) mod n ; k = (0,…,6)
(a/m)y mod (n/m)=1;

(7/7)y mod (21/7) = 1;   y mod 3 = 1;   y = 1
X_k = (3·1+k·13) mod 91 = (3 + 13·k) mod 91 , con k=(0,…,6)
K=0, x=3
K=1, x=16
K=2, x=29
K=3, x=42
K=4, x=55
K=5, x=68
K=6, x=81

B) 6·x=5 mod 43

SOLUCIÓN:
mcd (6, 43) = 1, existe solución y es única.
6y = 1 mod 43, aplicando Euclides,
43 = 6*7 + 1,
y= -7 mod 43 = 36

x = 5·36 mod 43 = 8

CRIPTOGRAFÍA Y SEGURIDAD INFORMÁTICA
GRADO EN INGENIERÍA INFORMÁTICA
Examen 1 Parcial Evaluación Continua Leganés/Colmenarejo – Semana 3 – 2016
Apellidos: **Nombre:**
Grupo **Modelo 3**

EJERCICIO 5 (0,2 puntos)

Encuentre dos raíces primitivas respecto al módulo 11.

Sol:

Hay $\Phi(10)= \Phi(2\cdot5)=4$ raíces primitivas módulo 11. No podría haber 6, por el mismo motivo.

Sabemos que el orden es divisor de p-1 = 10, por lo que los órdenes a considerar son {1,2,5,10}

2^1 mod 11 = 2 ; 2^2 mod 11 = 4 ; 2^5 mod 11 = 10 ; 2^{10} mod 11 = 1 , 2 es raíz primitiva
3^1 mod 11 = 3 ; 3^2 mod 11 = 9 ; 3^5 mod 11 = 1, 3 no es raíz primitiva
4^1 mod 11 = 4 ; 4^2 mod 11 = 5 ; 4^5 mod 11 = 1, 4 no es raíz primitiva
5^1 mod 11 = 5 ; 5^2 mod 11 = 3 ; 5^5 mod 11 = 1, 5 no es raíz primitiva
6^1 mod 11 = 6 ; 6^2 mod 11 = 3 ; 6^5 mod 11 = 10 ; 6^{10} mod 11 = 1 , 6 es raíz primitiva
7^1 mod 11 = 7 ; 7^2 mod 11 = 5 ; 7^5 mod 11 = 4 ; 7^{10} mod 11 = 1 , 7 es raíz primitiva
8^1 mod 11 = 8 ; 8^2 mod 11 = 9 ; 8^5 mod 11 = 10 ; 8^{10} mod 11 = 1 , 8 es raíz primitiva
No debemos buscar más, pues sabemos que ya no hay más.

EJERCICIO 6 (0,2 puntos)

Sean los polinomios a(x)=x+1 y b(x)= x pertenecientes a CG(2^3) siendo el mod (p(x)), donde p(x) = x^3+x+1. Calcule el polinomio c(x) = $a(x)^2\cdot b(x)^3$ mód p(x)

SOLUCIÓN:
$c(x)= (x^2+1)\cdot x^3 = x^5+ x^3 \bmod \mathbf{x^3+x+1} = x^2$

CRYPTOGRAPHY AND COMPUTER SECURITY
BACHELOR IN INFORMATICS ENGINEERING

Test 1 Continuous assessment — Leganés – Week 3 – 2016

Surname: — **Name:**

Group — **Model 1**

CRYPTOGRAPHY AND COMPUTER SECURITY
BACHELOR IN INFORMATICS ENGINEERING

Test 1 Continuous assessment — Leganés – Week 3 – 2016

Surname: — **Name:**

Group — **Model 1**

CRYPTOGRAPHY AND COMPUTER SECURITY
BACHELOR IN INFORMATICS ENGINEERING

Test 1 Continuous assessment — Leganés – Week 3 – 2016

Surname: **Name:**

Group **Model 1**

EXERCISE 1 (0.2 marks)

Inverse calculation using Euler's Theorem

A) $7 \cdot x \bmod 22 = 1$

SOL:

As gcd (7, 22) = 1, Euler can be applied. $\Phi(22) = \Phi(2) \cdot \Phi(11) = 10$

$x = ^{\Phi(n)-1} \bmod 22 = 7^{10-1} \bmod 22 = 7^9 \bmod 22 = 7\cdot(7^2)^4 \bmod 22 = 7\cdot 5^4 \bmod 22 = (7\cdot 3\cdot 3) \bmod 22 = 19$

Sol: x=19

B) $3 \cdot x \bmod 165 = 1$

SOL:

As gcd (3, 165) = 3, Euler's Theorem cannot be applied

EXERCISE 2 (0.2 marks)

Inverse calculation using Euclides' extended algorithm:

$61 \cdot x \bmod 197 = 1$

Sol:

$197 = 61 \cdot 3 + 14$
$61 = 14\cdot 4 + 5$
$14 = 5\cdot 2 + 4$
$5 = 4\cdot 1+1$

$1 = 5 – 4 = 5 – (14 – 5\cdot 2) = 3\cdot 5 – 14 = 3 \cdot (61 – 14\cdot 4) – 14 = 3\cdot 61 -13\cdot 14 = 3\cdot 61 - 13\cdot(197-3\cdot 61)=42\cdot 61 -13\cdot 197$

Sol: x = 42

EXERCISE 3 (0.1 marks)

Solve:

$11^{4200} \bmod 6125 = x$

Sol:

$6125= 5^3\cdot 7^2$, so

$\Phi(6125) = (5^{(3-1)}*(5-1))* (7^{(2-1)}*(7-1)) = (100)*(42) = 4200$

Given that gcd(11,6125) = 1, using Euler, $a^{\Phi(n)} \bmod n = 1$

Solución: x=1

CRYPTOGRAPHY AND COMPUTER SECURITY
BACHELOR IN INFORMATICS ENGINEERING

Test 1 Continuous assessment Leganés – Week 3 – 2016

Surname: **Name:**

Group **Model 1**

EXERCISE 3 (0.2 marks)

Equations of type a·x ≡ b mód n

A) 7·x=21 mod 28

SOL:
gcd (7, 28) = 7 and 7 divides 21, so there are 7 solutions, being a=7, b=21, n=28 and m=7:
x_k= (b/m)y+k(n/m) mod n ; k = (0…6)
(a/m)y mod (n/m)=1;

(7/7)y mod (28/7)=1; y mod 4 =1 ; y=1
X_k= 3·1+k·4 mod 28 , so:
Solutions:
K=0, x=3
K=1, x=7
K=2, x=11
K=3, x=15
K=4, x=19
K=5, x=23
K=6, x=27

B) 31·x=12 mod79

SOL: gcd (31, 79) = 1, there is one solution:
31y mod 79 = 1, using Euclides,

79 = 31·2+17

31= 17 · 1 + 14

17 = 14 ·1 + 3

14 = 3·4 + 2

3=2 + 1

1= 3-2=3-(14-3·4)=5·3-14=5·(17-14)-14=5·17-6·14=5·17-6·(31-17)=11·17-6·31=

11·(79-2·31)-6·31=11·79-28·31,

y=-28 mod 79 = 51

x = 51 ·12 mod 79 = 612 mod 79 = 59

CRYPTOGRAPHY AND COMPUTER SECURITY
BACHELOR IN INFORMATICS ENGINEERING

Test 1 Continuous assessment — Leganés – Week 3 – 2016

Surname: **Name:**

Group **Model 1**

EXERCISE 5 (0.1 marks)

Explain in detail whether the following statement is true or false:

There are 8 primitive roots mod 31

Compute one primitive root respect to modulo 31.

Sol: As p=31 is prime, there are $\Phi(p-1)= \Phi(30)= \Phi(2\cdot 3\cdot 5)=8$ primitive roots. The statement is true

EXERCISE 6 (0.2 marks)

Carry out the following operations with polynomials belonging to $GF(2^4)$, in which the irreducible polynomial is $p(x) = x^4+x+1$.

A) Considering $a(x) =(x^3+x^2)$, calculate $a(x)^2 \bmod p(x)$

Sol: $a(x)^2 = x^6+x^4$ in $GF(2^4)$, so,
$x^6+x^4 \bmod x^4+x+1 = x^3+x^2 +x+1$

CRYPTOGRAPHY AND COMPUTER SECURITY
BACHELOR IN INFORMATICS ENGINEERING

Test 1 Continuous assessment — Leganés – Week 3 – 2016

Surname: — **Name:**

Group — **Model 2**

EXERCISE 1 (0.2 marks)

Inverse calculation using Euler's Theorem

A) $9 \cdot x \bmod 41 = 1$

SOL:

As gcd (9, 41) = 1 , Euler can be applied. Given that $\Phi(41) = 40$

$x=9^{\Phi(41)-1} \bmod 41 = 9^{39} \bmod 41 = 9\cdot(9^2)^{19} \bmod 41 = 9\cdot(-1)^{19} \bmod 41 = -9 \bmod 41 = 32$

Sol: x=32

B) $7 \cdot x \bmod 72 = 1$

SOL:

As gcd (7, 72) = 1 Euler can be applied. As $72=3^2 \cdot 2^3$, $\Phi(72) =(3^{2-1}\cdot(3-1))*(2^{3-1}\cdot(2-1))=6\cdot4=24$

$x=7^{\Phi(72)-1} \bmod 72 = 7^{23} \bmod 72 = 49 \cdot (7^3)^7 \bmod 72 = 49 \cdot 55^7 \bmod 72 = 49 \cdot 55 \bmod 72 = 31$

Sol: x=31

EXERCISE 2 (0.2 marks)

Inverse calculation using Euclides' extended algorithm:

$23 \cdot x \bmod 47 = 1$

Sol:

$47=23\cdot2+1$

$x = -2 = 45 \bmod 47$

CRYPTOGRAPHY AND COMPUTER SECURITY
BACHELOR IN INFORMATICS ENGINEERING

Test 1 Continuous assessment — Leganés – Week 3 – 2016

Surname: **Name:**

Group **Model 2**

EXERCISE 3 (0.1 marks)

Explain if there is a number "s" such that

3^s mod 13 = 1

If "s" exists, explain how many of them may exist. Based on the previous facts, is 3 primitive root of 13?

SOL:
Yes, there is such a number since gcd(3,13)=1. Thus, at least based on Euler, s=Φ(13)=12.
All numbers "s" satisfying such condition are divisors of p-1=12. These divisors are {1,2,3,4,6,12}. Therefore:
3 mod 13 = 3
9 mod 13 = 9
27 mod 13 = 1 , so s=3 is also valid. This implies that 3 is not primitive root of 13.

EXERCISE 4 (0.2 marks)

Equations type a·x ≡ b mód n

A) 19·x=20 mod 37

SOL:
gcd (19, 37) = 1, unique solution:

19y mod 37 = 1, using Euclides:
37= 19 ·1 + 18
19=18 + 1,
1= 19-18=19-(37-19)=2·19-37 , de lo que y=2
x=20y mod 37 = 40 mod 37 = 3

B) 15·x=12 mod 21

SOL:
gcd (15, 21) = 3 and 3 divides 12, so there are 3 solutions, with k=0,1,2 , a=15, b=12, n=21 and m=3,
x_k= (b/m)y + k(n/m) mod n ; k = (0,1,2)
(a/m)y mod (n/m)=1;

(15/3)y mod (21/3) = 1; 5y mod 7 = 1; y = 3
X_k = (4·3+k·7) mod 21 = (12 + 7·k) mod 21 , with k=(0,1,2)

Sol: x_k = (12,19,5)

EXERCISE 5 (0.1 marks)

How many positive numbers, below 3267, are relatively primes to it?

Sol: $\Phi(3267)= \Phi(11^2 \cdot 3^3)=(11^{2-1} \cdot (11-1)) \cdot (3^{3-1}(3-1))=(110) \cdot 18=1980$

EXERCISE 6 (0.2 marks)

Let $a(x)=x^2+1$ and $b(x)= x^2$ from $GF(2^3)$, with mod $(p(x))$, where $p(x) = x^3+x+1$. Calculate the polynomial $c(x) = a(x)^2 \cdot b(x) \bmod p(x)$

SOL:
$c(x)= (x^4+1) \cdot x^2 = x^6+ x^2 \bmod \mathbf{x^3+x+1} = 1$