# Mathematical background

## CRYPTOGRAPHY AND COMPUTER SECURITY

Ana I. González-Tablas Ferreres
José María de Fuentes García-Romero de Tejada
Lorena González Manzano
Sergio Pastrana Portillo

uc3m | Universidad Carlos III de Madrid

COSEC

# OUTLINE

- 1. Mathematical background
  - Basic concepts
    - Congruence
    - Modular reduction
    - $Z_n$ set
  - Inverse computation
    - Fermat's theorem
    - Euler Totient Function
    - Euler's theorem
    - Inverse computation by means of Extended Euclidean Algorithm
  - Congruence equations
    - Powers of an integer
    - Primitive roots
    - Discrete logarithms



Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana

# OUTLINE

- 1. Mathematical background
  - Basic concepts
    - Congruence
    - Modular reduction
    - $Z_n$ set
  - Inverse computation
    - Fermat's theorem
    - Euler Totient Function
    - Euler's theorem
    - Inverse computation by means of Extended Euclidean Algorithm
  - Congruence equations
    - Powers of an integer
    - Primitive roots
    - Discrete logarithms



Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana

# MATHEMATICAL BACKGROUND

- Basic concepts
  - Let **Z** be the set of integers and a, b, c ∈ **Z**
    - (**Z**, +) qualifies as a group if:

| | |
|---|---|
| $a + b \in \mathbf{Z}$ | closure |
| $a + (b + c) = (a + b) + c$ | associativity |
| $a + 0 = a$ | identity element |
| $a + (-a) = 0$ | inverse element |


Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana

# MATHEMATICAL BACKGROUND

- (**Z**, +) qualifies as an abelian group if:

| | |
|---|---|
| $a + b = b + a$ | commutativity (abelian) |

- (**Z**, +, ·) qualifies as a ring if (**Z**, +) is and abelian group and:

| | |
|---|---|
| $a \cdot b \in \mathbf{Z}$ | closure |
| $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ | associativity |
| $a \cdot I = a$ | identity element |
| $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ | · distributivity over + |

Closure, associativity and identity element: (**Z**, ·) monoid



Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana

# MATHEMATICAL BACKGROUND

- (**Z**, +, ·) qualifies as a commutative ring if:

| | |
|---|---|
| $a \cdot b = b \cdot a$ | conmutativity |

- (**Z**, +, ·) is a field if it is a commutative ring and posseses a multiplicative inverse:

| | |
|---|---|
| $a \cdot a^{-1} = 1$ | Inverse element ( ·) |



Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana

# OUTLINE

- 1. Mathematical background
  - Basic concepts
    - Congruence
    - Modular reduction
    - $Z_n$ set
  - Inverse computation
    - Fermat's theorem
    - Euler Totient Function
    - Euler's theorem
    - Inverse computation by means of Extended Euclidean Algorithm
  - Congruence equations
    - Powers of an integer
    - Primitive roots
    - Discrete logarithms



Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana

# CONGRUENCE RELATIONSHIP

- For a positive integer *n*, two integers *a* and *b* are said to be **congruent modulo** *n*, written:

  $a \equiv b \bmod n \Leftrightarrow (a - b)$ is an integer multiple of *n*.

- The number *n* is called the **modulus** of the congruence.

- An equivalent definition is that both numbers have the same remainder when divided by *n*.

- (mod n) operator maps all integers into the set {0,1,…,n-1}



Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana

# CONGRUENCE CLASSES

- We denotate [a] to the set {..., a-2n, a-n, a, a+n, a+2n, ...}, that is the congruence class of a modulo n (that is, for all x, y ∈ [a] regarding n, x ≡ y (mod.n) y a ∈ {0,1,...n-1})

The congruence class [3] modulo 10 =

$[3]_{10}$ = { ..., -27, -17, -7, 3, 13, 23, 33, ...} =
{ ..., 3 – **3**·10, 3 – **2**·10, 3 – **1**·10, 3 – **0**·10, 3 + **1**·10, 3 + **2**·10, 3 + **3**·10,...}
-27 ≡ -17 ≡ -7 ≡ 3 ≡ 13 ≡ 23 ≡ 33 (mod.10)

The congruence class [7] modulo 11 =

$[7]_{11}$ = { ..., -26, -15, -4, 7, 18, 29, 40, ...} =
{ ..., 7 – **3**·11, 7 – **2**·11, 7 – **1**·11, 7 – **0**·11, 7 + **1**·11, 7 + **2**·11, 7 + **3**·11,...}
-26 ≡ -15 ≡ -4 ≡ 7 ≡ 18 ≡ 29 ≡ 40 (mod.11)



Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana

# OUTLINE

- 1. Mathematical background
  - Basic concepts
    - Congruence
    - Modular reduction
    - $Z_n$ set
  - Inverse computation
    - Fermat's theorem
    - Euler Totient Function
    - Euler's theorem
    - Inverse computation by means of Extended Euclidean Algorithm
  - Congruence equations
    - Powers of an integer
    - Primitive roots
    - Discrete logarithms





Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana

# MODULAR REDUCTION

Given $a$, n ∈ **Z** (n ≠ 0). Modular reduction (or modulo n) is called to the function (represented by (mod. n)) that applying to $a$, the result is r ∈ $\mathbf{Z}^+ + \{0\}$ / r ∈ {0,1,...n-1} and $a \equiv$ r (mod. n)

$$a \text{ (mod. n)} = r \Rightarrow a \equiv r \text{ (mod. n) and } r \in \{0,1,\ldots n-1\}$$

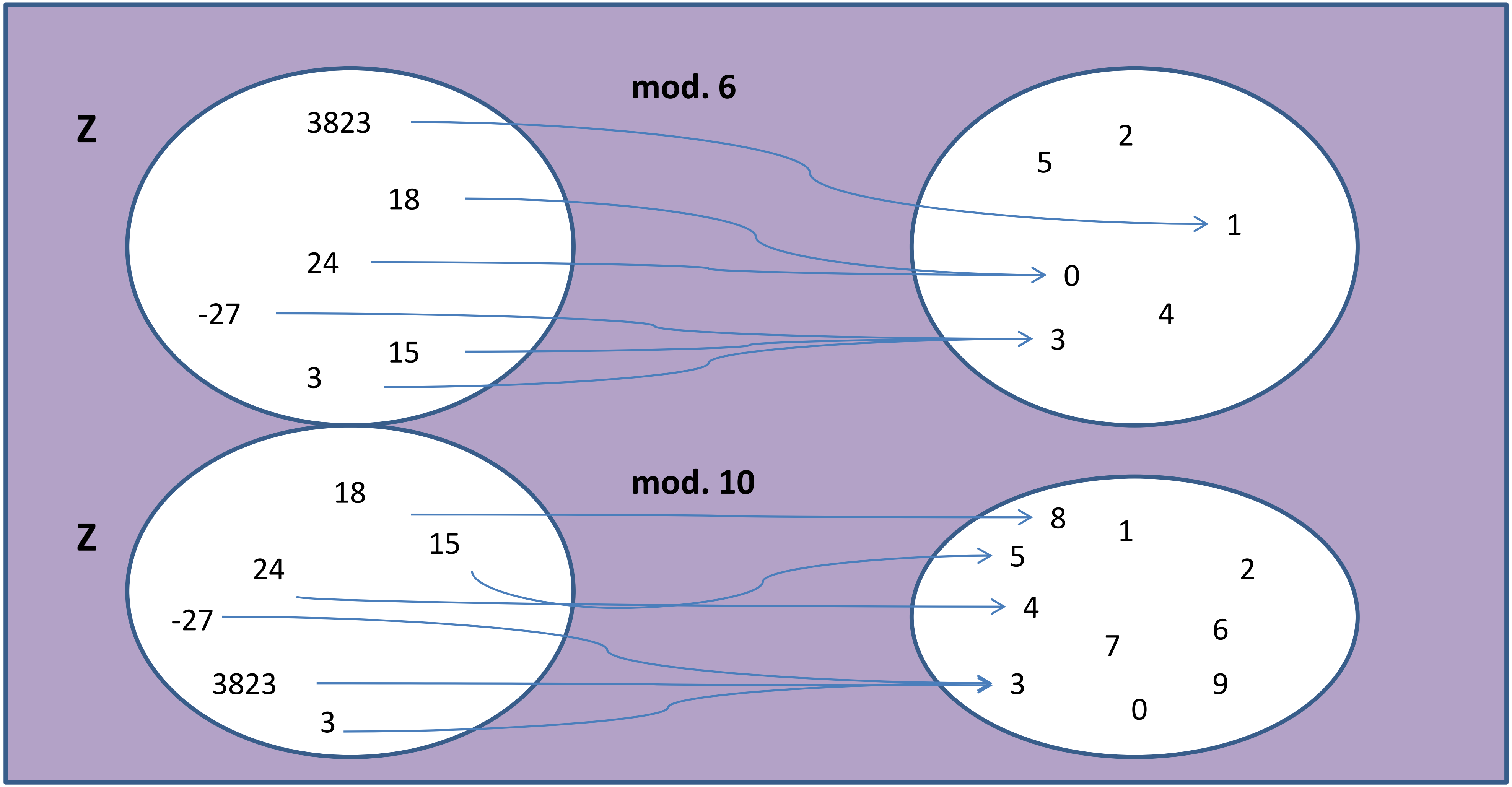
Note: "r is the reminder of the integer division of $a$ between n (for $a > 0$)"

26 (mod. 5) = 5 · 5 + 1 (mod. 5) = 1 (1<5-1) 26 ≡ 1 (mod. 5)
30 (mod. 7) = 4 · 7 + 2 (mod. 7) = 2 (2<7-1) 30 ≡ 2 (mod. 7)
11 (mod. 33) = 11 (11<33-1)
256 (mod. 8) = 32·8+0 (mod. 8) = 0 (0<8-1) 256 ≡ 0 (mod. 8)
-17 (mod. 12) ≡ -17 + 2 · 12 = 7 (7<12-1) -17 ≡ 7 (mod. 12)



Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana

# MODULAR REDUCTION



# OUTLINE

- 1. Mathematical background
  - Basic concepts
    - Congruence
    - Modular reduction
    - $Z_n$ set
  - Inverse computation
    - Fermat's theorem
    - Euler Totient Function
    - Euler's theorem
    - Inverse computation by means of Extended Euclidean Algorithm
  - Congruence equations
    - Powers of an integer
    - Primitive roots
    - Discrete logarithms



Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana

# $Z_n$ SET

– $Z_n = \{ [a] \, / \, a \in Z \}$

$Z_n$ is the set of congruence classes regarding a modulo n

If $n \neq 0$, $Z_n = \{[0], [1], \ldots [n-1]\}$ or simplified

$Z_n = \{0, 1, \ldots n-1\}$ ("**the ring of integers modulo n**")

$Z_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$

$Z_{31} = \{0, 1, 2, 3, 4, 5, 6, 7, \ldots, 26, 27, 28, 29, 30\}$



Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana

# $Z_n$ SET

- **Operations ($+_n$, $\cdot_n$)**
  - Addition and multiplication is defined for $\mathbf{Z_n}$

For [a], [b], [c] $\in \mathbf{Z}_n$

$+_n$ : $[a] +_n [b] = [a+b]$

$\cdot_n$ : $[a] \cdot_n [b] = [a \cdot b]$

$Z_8$ :

$[6] +_8 [7] = (6 + 7)$ mod. 8 = 13 mod. 8 = [5]

$Z_{31}$ :

$[3] \cdot_{31} [11] = (3 \cdot 11)$ mod. 31 = 33 mod. 31 = [2]



Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana

# $Z_n$ SET

– **$Z_n$ - properties regarding ($+_n$, $\cdot_n$)**

For $n \neq 0$, $Z_n$ is a computative ring regarding ($+_n$, $\cdot_n$)

| | |
|---|---|
| $[a] +_n [b] \in \mathbf{Z}_n$ | $[a] \cdot_n [b] \in \mathbf{Z}_n$ |
| $[a] +_n ([b] +_n [c]) = ([a] +_n [b]) +_n [c]$ | $[a] \cdot_n ([b] \cdot_n [c]) = ([a] \cdot_n [b]) \cdot_n [c]$ |
| $[a] +_n 0 = [a]$ | $[a] \cdot_n 1 = [a]$ |
| $[a] +_n (-[a]) = 0$ | $[a] \cdot_n ([b] +_n [c]) = ([a] \cdot_n [b]) +_n ([a] \cdot_n [c])$ |
| $[a] +_n [b] = [b] +_n [a]$ | $[a] \cdot_n [b] = [b] \cdot_n [a]$ |



Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana

# $Z_n$ SET

- Homomorphism relationship with Z ring of integers
- Function “Modular reduction” is an homomorphism between Z (ring of integers) and **$Z_n$** (ring of integers modulo n) <-> It is verified that:

Given a, b $\in$Z, f(a),f(b) $\in Z_n$, with f: Z ---> $Z_n$ (f = Modular reduction)

$f(a + b) = f(a) +_n f(b)$ ; $f(a \cdot b) = f(a) \cdot_n f(b)$

- “Consequences” (Fundamental principles of modular arithmetic):
  - **(a + b) (mod. n)** = a (mod. n) $+_n$ b (mod. n) = (a(mod. n) + b(mod. n))(mod. n)

    $[ (a + b) ] = [a] +_n [b] = [ [a] + [b] ]$
  - **(a·b) (mod. n)** = a (mod. n) $\cdot_n$ b (mod. n) = (a (mod. n) · b (mod. n)) (mod. n)

    $[ (a \cdot b) ] = [a] \cdot_n [b] = [ [a] \cdot [b] ]$
  - **(a·(b+c)) (mod. n)** = ((a (mod. n) $\cdot_n$ b (mod. n)) $+_n$ (a (mod. n) $\cdot_n$ c (mod. n)) =

    = ((a· b) (mod. n)+(a·c) (mod. n)) (mod. n)

    $[ (a \cdot (b + c)) ] = [a] \cdot_n ( [b] +_n [c] ) = [ [a] \cdot ( [b] + [c] ) ]$

examples




Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana

# MATH FUNDAMENTALS

**(a + b)(mod. n)** = a (mod. n) $+_n$ b (mod. n) = (a(mod. n) + b(mod. n))(mod. n)

[ (a + b) ] = [a] $+_n$ [b] = [ [a] + [b] ]

Example:

**(3 + 8) (mod. 5)** = 3 (mod. 5) $+_n$ 8 (mod. 5) =

= (3 (mod. 5) + 8 (mod. 5)) mod. 5 =

= ( 3 + 3 ) mod. 5 = 6 mod. 5 = **1**

**(3 + 8) (mod. 5) =** 11 (mod. 5) = 1




Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana

# MATH FUNDAMENTALS

**(a·b)(mod. n)** = a(mod. n) $\cdot_n$ b(mod. n) = (a(mod. n) · b(mod. n))(mod. n)

[ (a · b) ] = [a] $\cdot_n$ [b] = [ [a] · [b] ]

Example:

**(3 · 8) (mod. 5)** = 3 (mod. 5) $\cdot_n$ 8 (mod. 5) = ( 3 (mod. 5) · 8 (mod. 5) ) mod. 5 =

= ( 3 · 3 ) mod. 5 = 9 mod. 5 = **4**

**(3 · 8) (mod. 5)** = 24 (mod. 5) = 4

**$7^4$ (mod. 5)** = (7 · 7 · 7 · 7) (mod. 5) =

= ( 7 (mod. 5) · 7 (mod. 5) · 7 (mod. 5) · 7 (mod. 5) ) mod. 5 =>>

= ( 2 · 2 · 2 · 2) mod. 5 = $2^4$ (mod. 5) = 16 mod. 5 = **1**

**$7^4$ (mod. 5)** = 2401 (mod. 5) = 1







Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana

# MATH FUNDAMENTALS

**(a· (b+c))(mod. n)** $= ((a(\text{mod. } n) \cdot_n b(\text{mod. } n)) +_n (a(\text{mod. } n) \cdot_n c(\text{mod. } n)) =$

$=((a\cdot b)(\text{mod. } n) + (a\cdot c)(\text{mod. } n))(\text{mod. } n)$

$[\ (a \cdot (b + c))\ ] = [a] \cdot_n (\ [b] +_n [c]\ ) = [\ [a] \cdot (\ [b] + [c]\ )\ ]$

Example:

**(3· (8+4))(mod. 5)** $= ((3(\text{mod. } 5) \cdot_n 8(\text{mod. } 5)) +_n (3(\text{mod. } 5) \cdot_n 4(\text{mod. } 5)) =$

$= ((3 \cdot 8)(\text{mod. } 5) + (3\cdot 4)(\text{mod. } 5))(\text{mod. } 5) =$

$= ((3 \cdot 3)(\text{mod. } 5) + (3\cdot 4)(\text{mod. } 5))(\text{mod. } 5) =$

$= (9\ (\text{mod. } 5) + 12\ (\text{mod. } 5))\ (\text{mod. } 5) = (4 + 2)\ (\text{mod. } 5) =$

$= 6 \text{ mod. } 5 =$ **1**

**(3· (8+4))(mod. 5)** $= 36\ (\text{mod. } 5) = 1$



Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana

# MATH FUNDAMENTALS

More examples:

**$(23 + 4)(\text{mod. } 5) = 2$**

**$2^9 (\text{mod. } 5) = 2$**

**$(3 + 8) \cdot 5 (\text{mod. } 5) = 0$**

**$(41 + 1001) \cdot 999 (\text{mod. } 5) = 3$**







Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana

# OUTLINE

- 1. Mathematical background
  - Basic concepts
    - Congruence
    - Modular reduction
    - $Z_n$ set
  - Inverse computation
    - Fermat's theorem
    - Euler Totient Function
    - Euler's theorem
    - Inverse computation by means of Extended Euclidean Algorithm
  - Congruence equations
    - Powers of an integer
    - Primitive roots
    - Discrete logarithms




Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana

# FERMAT'S THEOREM

If p is a prime, $\forall$ a $\in$ **Z** / g.c.d. (a, p) = 1 then:

$$a^{p-1} \text{ mod. } p = 1$$

- $a*a^{p-2} = 1 \pmod p$, so $a^{p-2}$ is the inverse of a (mod p)
- Also known as Fermat's Little Theorem
- Also: $a^p = a \pmod p$
- Useful in public key and primality testing



Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana

# COMPUTING THE INVERSE. FERMAT'S THEOREM

- Compute: $2x \bmod 7 = 1$

  **Solution:**

  a=2, p=7 prime, g.c.d.(2,7)=1, applying Fermat:

  $x = 2^{p-2} \bmod 7 \Rightarrow x = 2^{7-2} \bmod 7 \Rightarrow x = 2^5 \bmod 7 \Rightarrow$

  $x = 2^3\, 2^2 \bmod 7 \Rightarrow x = 4 \bmod 7$

- Compute: $35x \bmod 3 = 1$

  **Solution**

  a=35, p=3 prime, g.c.d.(35,3)=1,

  $35x \bmod 3 = (35 \bmod 3)\,(x \bmod 3) \bmod 3 = 2x \bmod 3 = 1$

  applying Fermat: $x = 2^{p-2} \bmod 3 \Rightarrow x = 2^{3-2} \bmod 3 \Rightarrow x = 2$



Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana

# OUTLINE

- 1. Mathematical background
  - Basic concepts
    - Congruence
    - Modular reduction
    - $Z_n$ set
  - Inverse computation
    - Fermat's theorem
    - Euler Totient Function
    - Euler's theorem
    - Inverse computation by means of Extended Euclidean Algorithm
  - Congruence equations
    - Powers of an integer
    - Primitive roots
    - Discrete logarithms



Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana

# EULER TOTIENT FUNCTION Φ (N)

- **Reduced set of residues** ($Z_n^*$) is composed of numbers (residues) which are relatively prime to n
  - e.g. for n=10,
  - reduced set of residues is $Z_n^*$= {1,3,7,9}

- Number of elements (order) in reduced set of residues is called the **Euler Totient Function Φ(n)**



Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana

# EULER TOTIENT FUNCTION $\Phi$ (ℕ)

- **Computing $\Phi(n)$**
  - If p is prime

    $$\Phi(p) = p-1$$

  - If p is prime and $k \in \mathbf{Z}^+$:

    $$\Phi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$$

  - If p and q are relatively prime:

    $$\Phi(pq) = \Phi(p)\,\Phi(q)$$

  - If $n = \prod p_i^{k_i}$ / $\forall i$ $p_i$ is prime, $k_i \in \mathbf{Z}^+$:

    $$\Phi(n) = \prod p_i^{k_i-1}(p_i - 1)$$



Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana

# EULER TOTIENT FUNCTION Φ(N)

- Examples

$\Phi(37) = 36$

$\Phi(21) = (3-1)*(7-1) = 2*6 = 12$

$\Phi(172) = ?$



Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana

# OUTLINE

- 1. Mathematical background
  - Basic concepts
    - Congruence
    - Modular reduction
    - $Z_n$ set
  - Inverse computation
    - Fermat’s theorem
    - Euler Totient Function
    - Euler’s theorem
    - Inverse computation by means of Extended Euclidean Algorithm
  - Congruence equations
    - Powers of an integer
    - Primitive roots
    - Discrete logarithms



Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana

# EULER'S THEOREM

- **A generalization of Fermat's theorem**

$\forall$ a, n$\in$**Z** (n$\neq$0) / g.c.d.(a,n)=1:

$$a^{\Phi(n)} \mod. n = 1$$

so:

$$a\, a^{\Phi(n)-1} \mod. n = 1$$

$$a^{-1} = a^{\Phi(n)-1} \mod. n$$

- If n is prime (denoted as p):

$$a^{-1} = a^{p-2} \mod. p$$







Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana

# EULER'S THEOREM

– Examples

– *3x mod 10 = 1*

$a$=3; $n$=10; Φ(10)=4;

x = $3^{4-1}$ mod 10 = $3^3$ mod 10 = 3 $3^2$ mod 10

= 3 (-1) mod 10 =-3 mod 10 = 7

– *2x mod 11 = 1*

$a$=2; $n$=11; Φ(11)=10;

x = $2^{10-1}$ mod 11 = $(2^3)^3$ mod 11 = $(-3)^3$ mod 11 =

= (-2) (-3) mod 11 = 6



Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana

# COMPUTING THE INVERSE. EULER'S THEOREM. EXAMPLES:

- Compute: 37x mod.10 =1

**Solution**

a=37, n=10, g.c.d.(37,10)=1, 7x mod 10 =1

applying Euler: $x = 7^{\Phi(10)-1}$ mod.10

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

$x = 7^{4-1}$ mod.10 ⇨ $x = 7^{3}$ mod.10 ⇨ x = (-1) 7 mod.10 ⇨

x = -7 mod.10 ⇨ x = 3 mod.10 =3





Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana

# COMPUTING THE INVERSE. EULER'S THEOREM. EXAMPLES:

- Compute: 17x mod.12 =1

**Solution**

a=17, n=12, g.c.d.(17,12)=1, 5x mod 12 = 1

applying Euler: $x = 5^{\Phi(12) -1}$ mod.12

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

$x = 5^{4-1}$ mod.12 ⇨ $x = 5^3$ mod.12 ⇨ $x = 13 \cdot 5$ mod.12

⇨ x = 5





Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana

# COMPUTING THE INVERSE. EXAMPLES:

- Compute: 37x mod 41 =1

**Solution**

a=37, n=41, g.c.d.(37,41)=1,

applying Euler: $x = 37^{\Phi(41)-1} \mod 41$

…



Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana

# OUTLINE

- 1. Mathematical background
  - Basic concepts
    - Congruence
    - Modular reduction
    - $Z_n$ set
  - Inverse computation
    - Fermat's theorem
    - Euler Totient Function
    - Euler's theorem
    - Inverse computation by means of Extended Euclidean Algorithm
  - Congruence equations
    - Powers of an integer
    - Primitive roots
    - Discrete logarithms



Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana

# EUCLIDEAN ALGORITHM

- Determines the GCD of two integers.
- Its major significance is that it does not require factoring the two integers
- This technique can be used to compute the inverse of a number in modular arithmetic



Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana

# EUCLIDEAN ALGORITHM

- Example: Compute the gcd(1547,560)

| | | | | | | |
|---|---|---|---|---|---|---|
| | 2 | 1 | 3 | 4 | 1 | 3 |
| 1547 | 560 | 427 | 133 | 28 | 21 | 7 |
| 427 | 133 | 28 | 21 | **7** | **0** | |



Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana

# EUCLIDEAN ALGORITHM

- 1547 = 2 * 560 + 427
- 560 = 1 * 427 + 133
- 427 = 3 * 133 + 28
- 133 = 4 * 28 + 21
- 28 = 1 * 21 + 7
- 21 = 3 * 7 + 0
- gcd(1547,560) = 7



Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana

# EXTENDED EUCLIDEAN ALGORITHM

- **Computing inverses**

If gcd(a,n)=1

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | $c_1$ | $c_2$ | ... | ... | ... | $c_n$ | $r_{n-1}$ |
| n | a | $r_1$ | $r_2$ | ... | ... | $r_{n-1}$ | **1** |
| $r_1$ | $r_2$ | $r_3$ | ... | ... | **1** | **0** | |

$n = c_1 a + r_1$
$a = c_2 r_1 + r_2$
$r_1 = c_3 r_2 + r_3$
...
...
$r_{n-2} = c_n r_{n-1} + 1$
$r_{n-1} = c_{n+1} + 0$

Substituting:

$$1 = k_1 a + k_2 n$$

Reducing modulo n:

$$1 = k_1 a \text{ (mod. n)}$$

Then

$$k_1 = a^{-1} \text{ (mod. n)}$$



Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana

# EXTENDED EUCLIDEAN ALGORITHM

- 37x mod 41 =1

| | | | |
|---|---|---|---|
| | 1 | 9 | 4 |
| 41 | 37 | 4 | 1 |
| 4 | 1 | 0 | |

$n = c_1 a + r_1$ ⇨

$41 = 1 \cdot 37 + 4$

$37 = 9 \cdot 4 + 1$

$1 = 37 - 9 \cdot 4 = 37 - 9\,(41 - 37)$

$1 = 37 - 9 \cdot 41 + 9 \cdot 37 = 37 \cdot 10 - 9 \cdot 41$

$1 = 37\ 10 \bmod 41$

**x = 10 mod. 41**

# OUTLINE

- 1. Mathematical background
  - Basic concepts
    - Congruence
    - Modular reduction
    - $Z_n$ set
  - Inverse computation
    - Fermat's theorem
    - Euler Totient Function
    - Euler's theorem
    - Inverse computation by means of Extended Euclidean Algorithm
  - Congruence equations
    - Powers of an integer
    - Primitive roots
    - Discrete logarithms



Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana

# LINEAR CONGRUENCE EQUATIONS

$a\,x \equiv b \text{ mod. } n$ $\Rightarrow$ $a\,x + n\,k = b$

- If g.c.d.(a,n)=1,the eq. has a unique solution

$$a\,y = 1 \ (\text{mod. } n)\ \{y = a^{-1}\ (\text{mod. } n)\};\ \ x = b\,y\ (\text{mod. } n)$$

- If g.c.d.(a,n) = d $\neq$ 1, d | b, $\exists$ d solutions between 0 and d-1

$$x = (b/d)\,y + j\,(n/d) \bmod n \qquad j \in \{0, d-1\}$$

$$(a/d)\,y \bmod (n/d) = 1$$

- Else, there is no solution

# POWERS OF AN INTEGER, modulo n

- **a, n ∈ Z**

$a^0$ **mod. n**

$a^1$ **mod. n**

$a^2$ **mod. n**

**…**

$a^g$ **mod. n**



Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana

# OUTLINE

- 1. Mathematical background
  - Basic concepts
    - Congruence
    - Modular reduction
    - $Z_n$ set
  - Inverse computation
    - Fermat’s theorem
    - Euler Totient Function
    - Euler’s theorem
    - Inverse computation by means of Extended Euclidean Algorithm
  - Congruence equations
    - Powers of an integer
    - Primitive roots
    - Discrete logarithms



Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana

# PRIMITIVE ROOTS. GENERATOR

- From Euler's theorem $a^{\varnothing(n)} \bmod n = 1$
- Consider $a^g = 1 \pmod{n}$, $GCD(a,n)=1$
  - At least $g = \varnothing(n)$, but may be smaller
  - **Order** of a mod n is the least $g$ that holds eq.
  - if smallest $g$ is $g = \varnothing(n)$ then $a$ is called a **primitive root**



Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana

# PRIMITIVE ROOTS. GENERATOR

- Let p be a prime. If a $\in$ **Z**$^+$ and g.c.d.(a, p)=1, then

the order of a, ord(a), modulo p is a divisor of p - 1

- If p is prime and ord(a) = p - 1, then successive powers of a "generate" the group mod p ($Z_p$*)

There are $\Phi$ (p-1) primitive roots modulo p



Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana

# PRIMITIVE ROOTS. GENERATOR

- Compute the primitive roots of 7 ($Z_7$*)

$2^0 \equiv 1$, $2^1 \equiv 2$, $2^2 \equiv 4$, $2^3 \equiv 1$ g = 3

$3^0 \equiv 1$, $3^1 \equiv 3$, $3^2 \equiv 2$, $3^3 \equiv 6$, $3^4 \equiv 4$, $3^5 \equiv 5$, $3^6 \equiv 1$, g = 6

$4^0 \equiv 1$, $4^1 \equiv 4$, $4^2 \equiv 2$, $4^3 \equiv 1$ g = 3

$5^0 \equiv 1$, $5^1 \equiv 5$, $5^2 \equiv 4$, $5^3 \equiv 6$, $5^4 \equiv 2$, $5^5 \equiv 3$, $5^6 \equiv 1$ g = 6

$6^0 \equiv 1$, $6^1 \equiv 6$, $6^2 \equiv 1$ g = 2

- Solution: 3 and 5



Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana

# OUTLINE

- 1. Mathematical background
  - – Basic concepts
    - Congruence
    - Modular reduction
    - $Z_n$ set
  - – Inverse computation
    - Fermat’s theorem
    - Euler Totient Function
    - Euler’s theorem
    - Inverse computation by means of Extended Euclidean Algorithm
  - – Congruence equations
    - Powers of an integer
    - Primitive roots
    - Discrete logarithms



Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana

# DISCRETE LOGARITHM

- the inverse problem to exponentiation is to find the **discrete logarithm** of a number modulo n
- that is to find $x$ such that $b = a^x \pmod{n}$
- this is written as $x = \log_a b \pmod{n}$

- If a is a primitive root then it always exists, otherwise it may not, eg.

  $x = \log_3 4 \bmod 13$ has no answer

  $x = \log_2 3 \bmod 13 = 4$ by trying successive powers



Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana

# DISCRETE LOGARITHM

| $a$ | $a^2$ | $a^3$ | $a^4$ | $a^5$ | $a^6$ | $a^7$ | $a^8$ | $a^9$ | $a^{10}$ | $a^{11}$ | $a^{12}$ | $a^{13}$ | $a^{14}$ | $a^{15}$ | $a^{16}$ | $a^{17}$ | $a^{18}$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 3 | 9 | 8 | 5 | 15 | 7 | 2 | 6 | 18 | 16 | 10 | 11 | 14 | 4 | 12 | 17 | 13 | 1 |
| 4 | 16 | 7 | 9 | 17 | 11 | 6 | 5 | 1 | 4 | 16 | 7 | 9 | 17 | 11 | 6 | 5 | 1 |
| 7 | 11 | 1 | 7 | 11 | 1 | 7 | 11 | 1 | 7 | 11 | 1 | 7 | 11 | 1 | 7 | 11 | 1 |

- $x = \log_3 7 \bmod 19 = 6$ (3 is primitive root modulo 19)
- $x = \log_4 3 \bmod 19$ –There is not solution, 4 is not primitive root ($4^{¿x?} = 3$ mod. 19) but
- $x = \log_4 9 \bmod 19$ –There is solution but it is not unique x={4, 13}





Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana

CRYPTOGRAPHY AND COMPUTER SECURITY

COSEC

uc3m | Universidad Carlos III de Madrid