Introduction to Cryptology

Lecture-3

Mathematical Background :
A quick approach to Group and Field Theory

15.03.2023, v53

Mathematical Background

In Discrete Mathematics, Number Theory

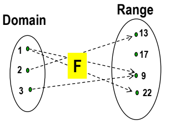
Outlines

Main Objectives for Crypto-Mappings/functions

Mapping function F :

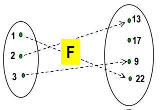
Domain: input choices

Range : Output choices



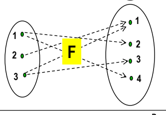
"One-To-One" functions:

No output from two different inputs



"Onto" functions:

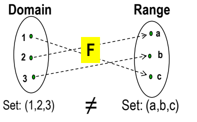
Every output results from at least one input
(scanning the input space would scan the whole output space)



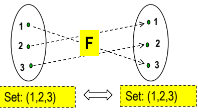
Targeted Crypto-Mappings

Bijective Function/Mapping :
IIs a mapping which is:
One-to-One AND Onto at the same time

- A function **F** has an inverse function F^{-1},
if and only if F is one to one



Permutation:
A **bijective function** from a set to itself is also called a **permutation** *(Domain = Range)*



Set: (1,2,3) ⟺ Set: (1,2,3)

Crypto-Mappings use mostly permutations to keep data size unchanged.
(domain space is the same as the range pace)

Number of permutations: **3!** = 3 x (3-1) x (3-2) = 6

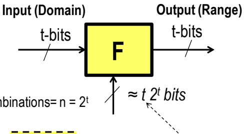
6 possible permutations
123 to 123
123 to 132
123 to 231
123 to 213
123 to 312
123 to 321

In general: |F| = Number of n to n permutations = n!

Permutations Bounds

Engineering approach:

Mapping as a hardware-block:



A mapping function from **t-bits to t-bits** keeping the input space=output space
(Data size unchanged!)

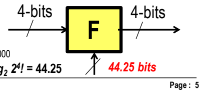
- Domain size = number of possible input combinations= $n = 2^t$
- Number of all possible "F" mappings = $2^{t\,2^t}$
- Number of all possible **invertible mappings** $S_{max} = 2^t\,!$

$\approx t\,2^t$ *bits*

Stirling's approximation $S_{max} = 2^t! \approx [\,2^t/e\,]^{2^t}$ or $S_{max} \approx 2^{(t-1.45)\,2^t}$

- Number of bits needed **to select all S_{max} mappings** = $\log_2 S_{max} = \log_2 2^t\,! \approx t\,2^t$ *bits*

Example: $t=4$, 4-bit to 4-bit mapping



Number of all possible mappings = $2^{4x16} = 2^{64}$ mappings
Number of possible invertible mappings = $2^4\,!$ = 20.922.789.888.000
 # bits required to select all possible invertible mappings = $\log_2 2^4! = 44.25$

Group Theory

Semigroup <S , *>

S ⇔ set of elements
* ⇔ operation
a * b = c , with a, b, c ∈ S (closure)
a * (b * c) = (a * b) * c , where a,b,c ∈ S (associative)

Monoid <M , *>

< M , * > ⇔ < S , * > in addition to a particular element **e**

- **e** is called the neutral element of the monoid with the properties:
e * a = a * e = a and a, e ∈ M
- **e** is unique
- an element ***a*** is invertible under * if there is b ∈ M such that:
a * b = b * a = e

b= a^{-1} is called **the inverse of a** under the Monoid operation * (the inverse b is unique)

Group <G, *>

- Is a Monoid, with **all *element are invertible*** under the operation * of G, that is:
  for any element **a** from G, there is **c** ∈ **G** such that : **c * a = e**, **($c = a^{-1}$)**

- If **a * b = b * a** then the group is called ***abelian*** (*or a **Commutative Group***)

!! Groups are the most used algebraic structures in cryptography !!

Examples:
Z is a group under *addition* where e=0 . The additive inverse of any b∈ **Z** is -b which also an element in **Z**

Z is however a Monoid under *multiplication* where e=1, as not every element has a multiplicative inverse (example there is no additive inverse for 2)

Ring <R, +, * >

<R, + > <=> abelian group with e=0
<R, *> <=> Monoid with e=1

The following holds:
a(b + c) = ab + ac
(b + c)a = ba + ca mit a,b, ∈ R

The Ring is ***commutative*** if:
a * b = b * a

Example: $\mathbf{Z_{10}}$ = {0,1,2,.....9} is the ring of integers modulo 10 with
⊕ : Addition modulo 10
⊙ : Multiplication modulo 10

Not all element in Z_m are invertible under multiplication
Example:
The Monoid Z_{10} under ⊙ (multiplication modulo 10)

where e=1, as a ⊙ e = e ⊙ a = a for a, e ∈ $\mathbf{Z_{10}}$

Invertible elements in < $\mathbf{Z_{10}}$, ⊙ > are:

1 ⊙ 1 = 1 => 1^{-1} = 1
3 ⊙ 7 = 1 => 3^{-1} = 7
9 ⊙ 9 = 1 => 9^{-1} = 9
7 ⊙ 3 = 1 => 7^{-1} = 3

1, 3, 7 and **9** are the only invertible elements in $\mathbf{Z_{10}}$

4 is not invertible as:
4 ⊙ 1 = 4
4 ⊙ 2 = 8
4 ⊙ 3 = 2
4 ⊙ 4 = 6
4 ⊙ 5 = 0
4 ⊙ 6 = 4
4 ⊙ 7 = 8
4 ⊙ 8 = 2
4 ⊙ 9 = 6
=> 4 has no inverse!

Invertible elements are called units

Reminder: Units and the Modular Multiplicative Inversion

***Definition:* If an integer is invertible under multiplication modulo m, then it is called a unit**

Example: ***2 x 3 = 6 = 1 (mod 5)***
says that : 3 is the multiplicative inverse of 2 modulo 5 (2^{-1}=3)
or 2 is the multiplicative inverse of 3 modulo 5 (3^{-1}=2)

Fundamental Theorem of units:
An integer **u** is a unit modulo m (or **u** has a ***multiplicative inverse*** **modulo m)** iff (if and only if):
$\boxed{\gcd(m, u) = 1}$

Computing the multiplicative inverse: If gcd (m, u) = 1 then **a.m + b.u = 1**
Taking the remainder modulo m of both sides: R_m (a m + b u) = R_m (1)
R_m (b . u) = 1
or R_m b • R_mu =1 => $\boxed{u^{-1} = R_m (b)}$
or $\boxed{u^{-1} = b \pmod m}$

That is the multiplicative inverse of *u mod m* is the parameter *b mod m* in the extended Euclidian gcd Algorithm.

Example: gcd (13, 2) = 1 = **1 . 13 - 6 . 2** *(Extended Euclidian Algorithm)*
R_{13}(1 . 13 – 6 . 2) = 1
R_{13}(-6 . 2) = 1 => $R_{13}(2^{-1})$ = -6 or -6 = -6+13 = 7 (mod 13)
That is **2^{-1} = -6 or 7** Check: 2 • -6 = -12 = 1 (mod 13) or 2 . 7 = 14 = 1 (mod 13)

The Group Z^*_m in Z_m

The (units) invertible elements under multiplication in Z_m build a group under multiplication this group is called Z^*_m

Example:
1, 3, 7 and **9** are the only invertible elements in $\mathbf{Z_{10}}$

==> Z^*_{10} = **{ 1, 3, 7, 9 } is a multiplicative group**

The neutral element is: e =1
The inverse of any element in Z^*_{10} is computable by the extended gcd algorithm

The number of elements in $\mathbf{Z^*_m}$ is called the order of the group $\mathbf{Z^*_m}$, the number is computable if m is possible to be factorized.
This number is known as **Euler Function ϕ(m)**

Invertible Elements and Euler Function ϕ(m)

For $\mathbf{m} = P_1^{e_1} P_2^{e_2} P_3^{e_3} \ldots P_t^{e_t}$ where $P_i \neq P_j$ for all i, j and P_i is a prime and e_i is a positive integer for any i.
The order of Z^*_m is called ***Euler Function ϕ(m)*** where:

$$\phi(m) = m \left(1 - \frac{1}{P_1}\right)\left(1 - \frac{1}{P_2}\right) \ldots \left(1 - \frac{1}{P_t}\right)$$

ϕ(m) : is the number of non-zero integers less than m and relatively prime to m
ϕ(m) represents therefore the number of invertible elements in Z_m.

Example 1: ϕ(15) = ϕ(5.3) =15 (1-1/5) (1-1/3)= (5-1)(3-1) = 8
(This means that only 8 integers modulo 15 have a multiplicative inverse. Which?)
Example 2: ϕ(45) = ϕ(5.3²) = 5.3² (1-1/5) (1-1/3)= 24

!! No technique is known to compute ϕ(m) without factoring m !!

Example: Number of units

The invertible elements (units) in $< Z_{15}, \odot >$ are all elements u for which
gcd (15, u) = 1

The number of units modulo 15 is : $\phi(15)$

compute $\phi(15)$:

15 is factored to 3 . 5 $\Rightarrow$ $\phi(15) = (3-1)(5-1) = \mathbf{8}$

The invertible elements are 1,2,4,7,8,11,13,14 , they build a group called Z^*_{15} with 8 elements.

To compute the multiplicative inverse any element in Z_m^*, the extended gcd algorithm is used as was shown in lecture 02

Galois*-Fields (Finite Fields) $GF \equiv <F, \oplus, \odot>$ * (Évariste Galois, 1811 –1832)

Set of elements **F** with two operations: Addition $\oplus$ and Multiplikation $\odot$ where :

Addition: $\oplus$
1. $(a \oplus b) \in F$ f a, b $\in F$ (closure)
2. $(a \oplus b) \oplus c = a \oplus (b \oplus c)$ (associative)
3. $a \oplus b = b \oplus a$ (commutative)

4. $\exists$ 0 in F (neutral element)
   such that $a \oplus 0 = 0 \oplus a = a$
5. $\exists$ -a in for any a in F (inverses Element)
   such that $a \oplus (-a) = (-a) \oplus a = 0$

Multiplication: $\odot$
1. $(a \odot b) \in F - \{0\}$ (closure)
2. $a \odot (b \odot c) = (a \odot b) \odot c$ (associative)
3. $a \odot b = b \odot a$ (commutative)

4. $\exists$ 1 in F (neutral element)
   such that $a \odot 1 = 1 \odot a = a$
5. $\exists$ a^{-1} for any $a \in (F - 0\})$ (inverses Element)
   such that $a \odot a^{-1} = a^{-1} \odot a = 1$ for all a, b $\in (F - \{0\})$

Addition / Multiplication: $\oplus$/$\odot$
1. $a \odot 0 = 0 \odot a = 0$
2. $a(b \oplus c) = ab \oplus ac$ (distributive)

For any prime number p there is a field having p elements.
Any non-zero element u from 1 to p-1 is invertible modulo p under multiplication.
(proof: As p is prime gcd (p,u)=1, thus every non-zero element has a multiplicative inverse)

Évariste Galois

October 25, 1811 – May 31, 1832 (lived 21 years!)

Académie des Sciences. First paper 17 years old
- **Cauchy, Fourier Poisson rejected his work**
- **His friend contacted Gauss and Jacobi after his death (no response is known)**
- **His achievements became first known after his death in 1843.**

"finite fields" are mostly known as „Galois Fields" GF

Basic intensive reference on GF:

R. Lidl and H. Niederreiter

Finite Fields
(Encyclopedia of Mathematics and its Applications)
Cambridge University Press, Cambridge, 1996.

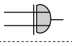
Galois-Field GF(2)

Example:
GF(2) = < {0, 1}; $\oplus$; $\odot$ >
with $\oplus$ as addition (mod 2) (**XOR**)
and $\odot$ as multiplication (mod 2) (**AND**).

Addition table

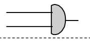
$\oplus$	0	1
0	0	1
1	1	0

!



Multiplication table

$\odot$	0	1
0	0	0
1	0	1



Galois-Field GF(3)

Example:
GF(3) = < {0, 1, 2}; $\oplus$; $\odot$ >
with $\oplus$ as addition (mod 3)
and $\odot$ as multiplication (mod 3)

Addition table

$\oplus$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

!

Multiplication table

$\odot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

!

Example: Arithmetic in Galois-Fields GF(7) $\Leftrightarrow$ $<F, \oplus, \odot>$

Example: Solve the set of linear equations in GF(7)

$4x_1 + x_2 = 3$ (1)
$2x_1 + 3x_2 = 4$ (2)

Gaussian reduction $2(4x_1 + x_2) = 3.2$ ($4^{-1} = 2$ in GF(7))
$x_1 + 2x_2 = 6 \rightarrow$ $x_1 = 6 - 2x_2$
replace in (2) $\rightarrow$ $2(6 - 2x_2) + 3x_2 = 4 \rightarrow -x_2 = -8$
$\rightarrow$ $x_2 = 1$ and $x_1 = 4$

AS Matrix:

$$\begin{bmatrix} 4 & 1 \\ 2 & 3 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 3 \\ 4 \end{bmatrix}$$

$$x_1 = \frac{\begin{vmatrix} 3 & 1 \\ 4 & 3 \end{vmatrix}}{\begin{vmatrix} 4 & 1 \\ 2 & 3 \end{vmatrix}} = \frac{(9-4)}{(12-2)} = \frac{5}{10} = \frac{5}{3} = 5.3^{-1} = 5.5 = 25 \equiv 4$$

$$x_2 = \frac{\begin{vmatrix} 4 & 3 \\ 2 & 4 \end{vmatrix}}{\begin{vmatrix} 4 & 1 \\ 2 & 3 \end{vmatrix}} = \frac{(16-6)}{(12-2)} = \frac{10}{10} = \frac{3}{3} = 1$$

Same example Arithmetic in Galois-Field GF(5) ⇔ <F, ⊕ , ⊙ >

Example: Solve the set of linear equations in GF(5)

$4 x_1 + x_2 = 3$ (1)
$2 x_1 + 3 x_2 = 4$ (2)

Gaussian reduction $4(4 x_1 + x_2) = 3 . 4$ [$4^{-1} = 4$ in GF(5)]
$x_1 + 4 x_2 = 2 \rightarrow x_1 = 2 - 4 x_2$

replace in (2) → $2(2 - 4 x_2) + 3 x_2 = 4$
→ $4 = 4$ The two equations are linearly dependent !!!

AS Matrix:

$$\begin{bmatrix} 4 & 1 \\ 2 & 3 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 3 \\ 4 \end{bmatrix} \Rightarrow$$

$$x_1 = \frac{\begin{vmatrix} 3 & 1 \\ 4 & 3 \end{vmatrix}}{\begin{vmatrix} 4 & 1 \\ 2 & 3 \end{vmatrix}} = \frac{(9 - 4)}{(12 - 2)} = \frac{5}{10} \equiv \frac{0}{0} \text{ !!!!}$$

$$x_2 = \frac{\begin{vmatrix} 4 & 3 \\ 2 & 4 \end{vmatrix}}{\begin{vmatrix} 4 & 1 \\ 2 & 3 \end{vmatrix}} = \frac{(16 - 6)}{(12 - 2)} = \frac{10}{10} \equiv \frac{0}{0} = ?\text{!!!!}$$

Order of a Group Elements

Let $\alpha \in$ < G, ⊙ >, the **order** of α is the **smallest n** such that:

$\underbrace{\alpha \odot \alpha \odot \ldots}_{\text{n-times}} = e$ or $\boxed{\alpha^n = e}$

⊙ : is the group operation,
e : is the neutral element

Example: powers of 5 in Z_7 = GF(7), 5^i : 5^1 5^2 5^3 5^4 5^5 5^6 =1
Elemets are 5 4 6 2 3 1 => order of 5 is 6

Fundamental properties of elements orders in a group:

Definition: The order of a group G is the number of its elements = |G|

- **(Lagrange Theorem): The order of any element in a finite group is finite and divides the group's order**

If the order of α is k then: $\boxed{\text{Ord}(\alpha^i) = k / \gcd(i,k)}$

A Cyclic Group

A cyclic group: Is a group that can be generated by one of its elements.

In a multiplicative group G:
If $\alpha \in$ G has the **order n** , and the elements : { α^1 α^2 α^3 .... α^n } build the whole group, then G is a cyclic group

The element which can generate the whole group is called a **primitive element**.
(not all elements can generate the whole group!)

Example: powers of 5 in Z_7 = GF(7) 5^1 5^2 5^3 5^4 5^5 5^6=1
Elemets are 5 4 6 2 3 1

Fundamental properties :
- **The number of elements with order k in a cyclic group is = ϕ(k)**
- **Element's order k always divides the group's order n (Lagrange Th.)**

Example: Order of Units in a Finite Field GF(7)

The invertible elements in < Z_7, ⊙ > are all non-zero elements for which
gcd (7, u) = 1
We have $\phi(7)=(7-1)= 6$ such invertible elements. The elements are 1,2,3,4,5,6. These elements build a cyclic multiplicative group. GF(7) = Z_7 *as 7 is a prime number.*.

The multiplicative order of any element should be a ***divisor of the group's oder=6*** .
Therefore, possible orders are then ***1,2,3, or 6***

Computing the order for any element, is by exponentiating it to **1, 2, 3 or 6.**
The smallest exponent yielding 1 modulo 7 is the element's order :
The order of 1 is 1 as $1^1 = 1$ in Z_7
The order of 2 is 3 as $2^3 = 8 = 1$ in Z_7
The order of 3 is 6 as $3^6 = 1$ in Z_7
The order of 4 is 3 as $4^3 = 1$ in Z_7
The order of 5 is 6 as $5^6 = 1$ in Z_7
The order of 6 is 2 as $6^2 = 1$ in Z_7

Example: Multiplicative orders of all non-zero elements in GF(7)

Primitive elements (field generators)

Element	1	2	3	4	5	6
Computing orders →	$1^1 = \underline{1}$	$2^1 = 2$ $2^2 = 4$ $2^3 = \underline{1}$	$3^1 = 3$ $3^2 = 2$ $3^3 = 6$ $3^4 = 4$ $3^5 = 5$ $3^6 = \underline{1}$	$4^1 = 4$ $4^2 = 2$ $4^3 = \underline{1}$	$5^1 = 5$ $5^2 = 4$ $5^3 = 6$ $5^4 = 2$ $5^5 = 3$ $5^6 = \underline{1}$	$6^1 = 6$ $6^2 = \underline{1}$
order	1	3	6	3	6	2

Facts:
- The order of any element should be a **divisor of 6**, that is **1,2,3, or 6**
- Number of elements from each order k is ϕ(k)
- The powers of the primitive elements 3 and 5 generate all non-zero elements of GF(7) (as a **Cyclic Group!**)

Example: Cyclic groups in GF(7)

Each element of order k generates a cyclic group having k elements

Element	1	2	3	4	5	6
Computing orders →	$1^1 = \underline{1}$	$2^1 = 2$ $2^2 = 4$ $2^3 = \underline{1}$	$3^1 = 3$ $3^2 = 2$ $3^3 = 6$ $3^4 = 4$ $3^5 = 5$ $3^6 = \underline{1}$	$4^1 = 4$ $4^2 = 2$ $4^3 = \underline{1}$	$5^1 = 5$ $5^2 = 4$ $5^3 = 6$ $5^4 = 2$ $5^5 = 3$ $5^6 = \underline{1}$	$6^1 = 6$ $6^2 = \underline{1}$

Cyclic group with **order 1**
Cyclic groups with **order 3**
Cyclic groups with **order 6**
Cyclic group with **order 2**

Divisors of $\phi(7)$= (7-1)

possible cyclic subgroup orders : **1, 2, 3, 6**

Order of any subgroup divides the group's order :

Summary: Order of elements in the Ring of Integers Modulo m: Z_m

The set of all units in Z_m build a **group** under multiplication called Z^*_m

Fundamental properties of the Z^*_m elements :

- **The multiplicative order of any element in Z^*_m divides $\phi(m)$**
- **If the order of α is k then** $Ord(\alpha^i) = k / gcd(i,k)$
  special case: If the order of α is k then the other elements with order k are (α^i) **for all i values for which** $gcd(i,k) = 1$
- **Number of elements with order k is = $\phi(k)$ if and only if Z^*_m is a cyclic group**

The **largest order** of a unit in Z^*_m is called $\lambda(m)$, known as Charmichael´s Function $\lambda(m)$

Largest multiplicative order of elements in Z^*_m

Carmicheal´s Function

The largest possible multiplicative order of an elements in Z^*_m is computable by **Carmichael´s function $\lambda(m)$:**

- $\lambda(m)$ divides $\phi(m)$
- **for any** $u \in Z^*_m$, $u^{\lambda(m)} = 1$ in Z_m , that is, the order of any unit divides $\lambda(m)$

Carmicheal´s function:

$\lambda(2) = 1$, $\lambda(2^2) = 2$, $\lambda(2^e) = 2^{e-2}$ for any $e \geq 3$:

$\lambda(p^e) = \Phi(p^e) = (p-1)p^{e-1}$ for p odd prim.

for $m = p_1^{e1}\ p_2^{e2}\ p_3^{e3}\ \dots\ p_n^{en}$

$\lambda(m) = lcm[\lambda(p_1^{e1}), \lambda(p_2^{e2}), \dots \lambda(p_n^{en})]$

lcm: least common multiple

Notice: non units (non-invertible elements) have no multiplicative order! Mathematically said to have order= ∞

hint

$$\mathrm{lcm}(a,b) = \frac{a \cdot b}{\gcd(a,b)}.$$

Example: multiplicative order of units in Z^*_{19} = GF(19)

- All non-zero elements are units or invertible as the modulus m=19 is a prime number
- The *Multiplicative Order* of any unit α in Z_{19} is a divisor of $\phi(19)$
- $\phi(19) = (19-1) = 18$
  we have 18 units (1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18)

- The multiplicative order of any unit is: 1, 2, 3, 6, 9, or 18 (i.e all divisors of 18)
  - from order 1 there are $\phi(1) = 1$ units
  - from order 2 there are $\phi(2) = 1$ units
  - from order 3 there are $\phi(3) = 2$ units
  - from order 6 there are $\phi(6) = (3-1)(2-1) = 2$ units
  - from order 9 there are $\phi(9) = \phi(3^2) = 3^2(1-1/3) = 6$ units
  - from order 18 there are $\phi(18) = \phi(2.3^2) = 18(1-1/2)(1-1/3) = 6$ units

- Find the order of the unit $\alpha = 2$:
  $2^1 = 2 \neq 1$, $2^2 = 4 \neq 1$, $2^3 = 8 \neq 1$, $2^6 = 7 \neq 1$, $2^9 = 18 \neq 1 \Rightarrow 2^{18} = 1$
  the order of 2 is 18 (2 is a primitive element)
  The other units with order 18 are: $2^1, 2^5, 2^7, 2^{11}, 2^{13}, 2^{17}$
  (1 ,5 ,7 ,11 ,13 ,17 are relatively prime to 18) $\downarrow$ 2 , 13, 14, 15 , 3 , 10

Useful fact:
$Ord(\alpha^i) = k / gcd(i,k)$

Example cont.: multiplicative order of units in Z^*_{19}

The fact that : $\boxed{Ord(\alpha^i) = k / gcd(i,k)}$ allows finding elements with other required orders:

- $Ord(2^{18}) = 18/gcd(18,18) = 1 \Rightarrow 2^{18} = 1$ has order 1
- $Ord(2^9) = 18/gcd(9,18) = 2 \Rightarrow 2^9 = 18$ has order 2
- $Ord(2^6) = 18/gcd(6,18) = 3 \Rightarrow 2^6 = 7$ has order 3
  the units with order 3 are: $7^1, 7^2$
  7 , 11
- $Ord(2^3) = 18/gcd(3,18) = 6 \Rightarrow 2^3 = 8$ has order 6
  the units with order 6 are: $8^1, 8^5$
  8 , 12
- $Ord(2^2) = 18/gcd(2,18) = 9 \Rightarrow 2^2 = 4$ has order 9
  the units with order 9 are: $4^1, 4^2, 4^4, 4^5, 4^7, 4^8$
  4 ,16 , 9, 17 , 6 , 5

Fermat and Euler's Theorems

Fermat´s Theorem: (Pierre de Fermat 1607- 1665)

- If m is a prime p then $\phi(m) = p-1$ for $1 \leq b < m$ $\Rightarrow$ $\boxed{b^{(p-1)} \equiv 1 \pmod p}$
- ***Primality test:*** If a number verifies Fermat theorem for some **b** then it is called a pseudo prime to the base **b**

Euler's Theorem: (Generalization of Fermat theorem): **Leonhard Euler:** 1707 Basel; † 1783 in Sankt Petersburg

If gcd (a, m) = 1
or for any unit **a** in Z_m or for any element in Z^*_m, the following holds:

$$\boxed{a^{\phi(m)} = 1 \quad (\text{in } Z_m)}$$

Proof: The order of any group's element $\alpha \in Z^*_m$ divides the group's order $\phi(m)$
Important Notice: the modulus in the exponent is $\phi(m)$ (example)