Let we have any set ***G*** (not necessary finite) consisting of the elements of any nature, i.e. ***G***={***a***, ***b***, ***c***, …, ***z***, …}.

1. ***Definition***. *A set **G** is an algebraic group if it is equipped with a binary operation • that satisfies four axioms:*

1. *Operation • is closed in the set;* for all ***a***, ***b***, there exists unique ***c*** in **G** *such that* ***a•b***=***c***.
2. *Operation • is associative; for all **a**, **b**, **c** in **G**: (**a•b**)•**c**=**a•**(**b•c**).*
3. *Group **G** has an neutral element abstractly we denote by **e** such that **a•e**=**e•a=a.***
4. *Any element **a** in **G** has its inverse* a^{-1} *with respect to • operation such that* $a \bullet a^{-1} = a^{-1} \bullet a = e$.

For curiosity, can be said that group axioms seems very simple but groups and their mappings describes a very deep and fundamental phenomena in physics and other sciences. Among these mappings a special importance have mappings preserving operations from one group to another called isomorphisms, or homomorphisms and morphisms in general. Isomorphisms have a great importance in cryptography to realize a secure confidential ***cloud computing***. It is named as ***computation with encrypted data***. The systems having a homomorphic property are named as ***homomorphic cryptographic systems***. They are under the development and are very useful in creation of secure e-voting systems, confidential transactions in blockchain and etc. We do not present there the construction of these systems and postpone it to the further issues of BOCTII, say in BOCTII.2. There we present one very important isomorphism example later when consider so called discrete exponent function (DEF).

T1. Theorem. If p is prime, then $Z_p^* = \{1, 2, 3, \ldots, p-1\}$ where operation is multiplication mod p is a multiplicative group.

Example: $p = 11 \Rightarrow Z_p^* = \{1, 2, 3, \ldots, 10\}$

Multiplication Tab. Z_{11}*										
*	1	2	3	4	5	6	7	8	9	10
1	1	2	3	4	5	6	7	8	9	10
2	2	4	6	8	10	1	3	5	7	9
3	3	6	9	1	4	7	10	2	5	8
4	4	8	1	5	9	2	6	10	3	7
5	5	10	4	9	3	8	2	7	1	6
6	6	1	7	2	8	3	9	4	10	5
7	7	3	10	6	2	9	5	1	8	4
8	8	5	2	10	7	4	1	9	6	3
9	9	7	5	3	1	10	8	6	4	2
10	10	9	8	7	6	5	4	3	2	1

$2 \cdot 6 = 12 \bmod 11 = 1$

$$\begin{array}{r|l} 12 & 11 \\ -11 & 1 \\ \hline 1 & \end{array}$$

$\left.\begin{array}{l} 4 \cdot 3 \bmod 11 = 12 \bmod 11 = 1 \\ 4 \cdot 4^{-1} \bmod 11 = (4/4) = 1 \end{array}\right\}$

$\Downarrow$

$4^{-1} = 3 \bmod 11$

$5 \cdot 9 = 45 \bmod 11 = 1$

$$\begin{array}{r|l} 45 & 11 \\ 44 & 4 \end{array}$$

10	10	9	8	7	6	5	4	3	2	1

$$\begin{array}{r|l} 45 & 11 \\ 44 & 4 \\ \hline 1 & \end{array}$$

```
>> mod(4*3,11)
ans = 1
>> mulinv(4,11)
ans = 3
```

7/4 mod 11 = 7*3 mod 11 = 10

$\overbrace{\hspace{10em}}^{x \in Z_{10}}$

Power Tab. Z_{11}*											
^	0	1	2	3	4	5	6	7	8	9	10
1	1	1	1	1	1	1	1	1	1	1	1
2	1	2	4	8	5	10	9	7	3	6	1
3	1	3	9	5	4	1	3	9	5	4	1
4	1	4	5	9	3	1	4	5	9	3	1
5	1	5	3	4	9	1	5	3	4	9	1
6	1	6	3	7	9	10	5	8	4	2	1
7	1	7	5	2	3	10	4	6	9	8	1
8	1	8	9	6	4	10	3	2	5	7	1
9	1	9	4	3	5	1	9	4	3	5	1
10	1	10	1	10	1	10	1	10	1	10	1

$Z_{11}^* = \{1, 2, 3, \ldots, 10\}$

$Z_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$

$DEF: Z_{10} \to Z_{11}^*$

$DEF_2(x) = 2^x \bmod 11 = a \in Z_{11}^*$

```
>> p=11;
>> g=2;
>> mod_exp(g,0,11)
ans = 1
>> mod_exp(g,1,11)
ans = 2
>> mod_exp(g,2,11)
ans = 4
>> mod_exp(g,3,11)
ans = 8
>> mod_exp(g,4,11)
ans = 5
```

```
>> mod_exp(g,10,11)
ans = 1
>> mod_exp(g,11,11)
ans = 2
>> mod_exp(g,12,11)
ans = 4
>> mod_exp(g,13,11)
ans = 8
>> mod_exp(g,14,11)
ans = 5
```

$$\left.\begin{array}{l} card(Z_{10}) = |Z_{10}| = 10 \\ Card(Z_{11}^*) = |Z_{11}^*| = 10 \end{array}\right\} \Rightarrow card(Z_{10}) = card(Z_{11}^*)$$

It is proved that:
if p is prime, then there exists such numbers g that $DEF_g(x)$ provides 1-to-1 or bijective mapping.

T2. Fermat (little)Theorem. If ***p*** is prime, then [Sakalauskas, at al.]

$$z^{p-1} = 1 \bmod p$$

$z \in Z_p^*$

$z^{p-1} = z^0 = 1 \bmod p$

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

How to find inverse element to z mod n?
>> mulinv(z,n)

Inverse elements in the Group of integers <Z_p^*, • mod p> can be found using either

How to find inverse element to z mod n?
>> mulinv(z,n)

Inverse elements in the Group of integers <$\mathbf{Z_p^*}$, $\bullet$ **mod** p> can be found using either Extended Euclidean algorithm or Fermat theorem, or ...

Let we have z in Z_p^*, then to find z^{-1} mod p it can be done by Octave:
>> z_m1=mulinv(z,p)

Let p is prime.
Then p is **strong prime** if $p=2q+1$ where $q = (p-1)/2$ is prime as well.
Then g in Z_P^* is a generator of Z_P^* if and only if
(**iff**) $g^2 \neq 1$ **mod** p **and** $g^q \neq 1$ **mod** p.

For example, let p is strong prime and $p=11$, then one of the generators is $g=2$.
Verification method: $g^2 \neq 1$ **mod** p **and** $g^q \neq 1$ **mod** p.
The main function used in cryptography is Discrete Exponent Function - DEF:
$\mathrm{DEF}_g(x) = g^x \bmod p = a$.

```
>> p=genstrongprime(28)
p = 144658379
>> isprime(p)
ans = 1
>> q=(p-1)/2
q = 72329189
>> isprime(q)
ans = 1
>> g=2;
>> mod_exp(g,2,p)
ans = 4
>> mod_exp(g,q,p)
ans = 144658378
```

Due to Fermat (little) theorem operations in exponents are perfoemed **mod** (p-1).
$g^{(a+b) \bmod (p-1)} \bmod p$

```
>> pp=11
pp = 11
>> gg=2
gg = 2
>> a=5
a = 5
>> b=9
b = 9
>> apb=mod(a+b,10)
apb = 4
>> g_apb=mod_exp(g,apb,11)
g_apb = 5
>> g_apb=mod_exp(g,14,11)
g_apb = 5
```