$\mathcal{Z} = \{\dots, -3, -2, -1, 0, 1, 2, \dots\}$

$\langle \mathcal{Z}, +, -, \cdot, / \rangle$; $\mathcal{Z}$ is closed with respect to $+, -, \cdot$ operations

$\mathcal{Z}$ - ring of integers

1. Closure $+, -, \cdot$
2. Associativity $\forall a, b, c \in \mathcal{Z} \rightarrow (a+b)+c = a+(b+c)$
   $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
3. „0" additively neutral element.
   $\forall a \in \mathcal{Z}: \quad a+0 = 0+a = a$
4. $\forall a \in \mathcal{Z} \rightarrow \exists! -a \in \mathcal{Z}: \quad a+(-a) = (-a)+a = 0$
   $-a$ is an additively inverse element.
5. „1" is a multiplicatively neutral element
   $\forall a \in \mathcal{Z}: \quad a \cdot 1 = 1 \cdot a = a$
6. Not all elements have multiplicatively inverse elem. such that $a \cdot \bar{a}^{-1} = \bar{a}^{-1} \cdot a = 1$ except element 1.
7. Distribution property
   $\forall a, b, c \in \mathcal{Z} \rightarrow a \cdot (b+c) = a \cdot b + a \cdot c$

Algorithm in $\mathcal{Z}$:

1. Greatest common Divider: >> gcd(a, n)

gcd(6, 15) = 3 gcd(10, 15) = 5

gcd(8, 15) = 1

If gcd(a, n) = 1, then a and n are relatively prime.

2. Extended Euklid Algorithm: >> eeuklid(a, n)

Operation modulo n: mod n.

Puz. 1. 137 mod 11 = 5

137 | 11
11 | 12

Ex. 1. $137 \bmod 11 = 5$

$137 = 12 \cdot 11 + 5$

137 | 11
11 | 12
27
22
5

Ex. 2. $n=2$: $\forall a \in \mathcal{Z} \rightarrow a \bmod 2 = \begin{cases} 0, \text{ if } a \text{ even} & (e) \\ 1, \text{ if } a \text{ odd} & (o) \end{cases}$

$a \bmod 2 \in \{0,1\}$

$\mathcal{Z} \bmod 2 = \{0,1\}$; $f_2 = \bmod 2 \rightarrow f_2(\mathcal{Z}) = \{0,1\} = \mathcal{Z}_2$

$f_2 : \mathcal{Z} \rightarrow \mathcal{Z}_2 = \{0,1\}$

$\mathcal{Z}_2$ arithmetics : $< \mathcal{Z}_2, \oplus, \& >$ (XOR, AND)

+	e	o
e	e	o
o	o	e

$e \equiv 0$, $o \equiv 1$

⊕	0	1
0	0	1
1	1	0

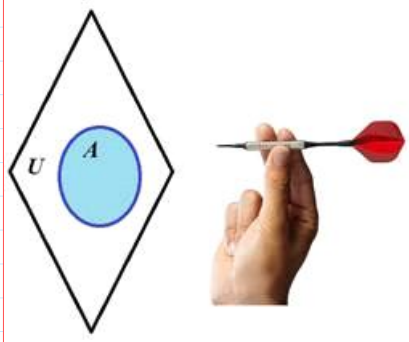
⊕ XOR Exclusive OR

·	e	o
e	e	e
o	e	o

$e \equiv 0$, $o \equiv 1$

&	0	1
0	0	0
1	0	1

& AND conjunction



XOR and AND logical operations in Boolean algebra can be illustrated by dartboard game.

Single Boolean variable can be represented by the set of 2 values {0,1} or {Yes,No} or {True,False}.

Let ***U*** is some universal set containing all other sets (we do not takke into account paradoxes related with ***U*** now).

Let ***A*** be a set in ***U***. Then with the set ***A*** in ***U*** can be associated a Boolean variable b_A=1 if area ***A*** is hit by missile

b_A=0 otherwise.

For this single variable b_A the negation (inverse) operation ` is defined:

$b_A^{\neg}$ =0 if b_A=1,

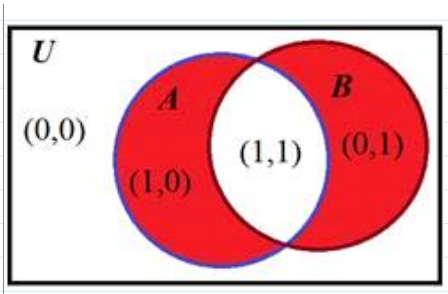
$b_A^{\neg}$ =1 if b_A=0.

Bollean operations are named also as Boolean functions.

Since negation operation/function is performed with the singe variable it is called a unary operation.

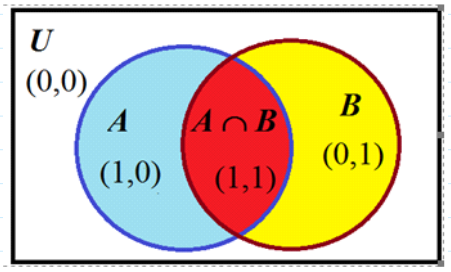
There are 16 Boolean functions defined for 2 variables and called binary functions.

Two of them XOR and AND are illustrated below.



A	B	A⊕B
0	0	0
1	0	1
0	1	1
1	1	0

A	B	A&B
0	0	0
1	0	0
0	1	0
1	1	1



Venn diagram of **A⊕B** operation.

Venn diagram of **A&B** operation.

$\langle \mathcal{I}, +, -, * \rangle$; $\langle \mathcal{I}_2, \oplus, \& \rangle$; $\mathcal{I}_2 = \{0,1\}$.

$a \in \mathcal{I}: a+0=a$; $a \in \mathcal{I}_2: a \oplus 0 = a$; ? $a-a=0$.

$\oplus$ - is additively selfinverse: $a-a = a \oplus a = 0$; $a \oplus b \oplus a = b \oplus 0 = b$.

$\mathcal{I}_3$ arithmetics: $\mathcal{I} \bmod 3 = \mathcal{I}_3 = \{0,1,2\}$

$(\mathcal{I}_{30} = \{0, 3, 6, 9, \dots\}) \bmod 3 = 0$

$(\mathcal{I}_{31} = \{1, 4, 7, 10, \dots\}) \bmod 3 = 1$

$(\mathcal{I}_{32} = \{2, 5, 8, 11, \dots\}) \bmod 3 = 2$

$8 \mid 3$; 6 ; 2

$7 \mid 3$; 6 ; 1

$12 \mid 3$; 12 ; 0

$\mathcal{I} = \mathcal{I}_{30} \cup \mathcal{I}_{31} \cup \mathcal{I}_{32}$; $\mathcal{I}_{30}, \mathcal{I}_{31}, \mathcal{I}_{32}$ – are not intersecting

$\mathcal{I}_n$ arithmetic ($n < \infty$): $\mathcal{I} \bmod n = \mathcal{I}_n = \{0,1,2,\dots,n-1\}$ ($|n$)

$\mathcal{I}_n$ is a ring with operations $+_{\bmod n}$ и $\cdot_{\bmod n}$

$\forall a,b \in \mathcal{I}_n$: $a +_{\bmod n} b = c \in \mathcal{I}_n$

$a \cdot_{\bmod n} b = d \in \mathcal{I}_n$

Inverse operat. $-_{\bmod n}$ $/_{\bmod n}$

$a + b = c \bmod n$

$a \cdot b = d \bmod n$

Operation properties:

$(a+b) \bmod n = (a \bmod n + b \bmod n) \bmod n$

$(a \cdot b) \bmod n = (a \bmod n \cdot b \bmod n) \bmod n$

$(a-b) \bmod n = \begin{cases} a-b, & \text{if } a \geq b \\ a+n-b, & \text{if } a < b \end{cases}$; $a,b < n$

$n \mid n$; n ; 0 $\Rightarrow$ $0 \equiv n \bmod n$

For given $b \in \mathcal{I}_n$. Find: $-b \in \mathcal{I}_n$: $b + (-b) \bmod n = 0 \in \mathcal{I}_n$

$a+n-b$, if $a<b$

For given $b \in \mathcal{Z}_n$. Find : $-b \in \mathcal{Z}_n$: $b+(-b) \bmod n = 0 \in \mathcal{Z}_n$

$-b \bmod n = (0-b) \bmod n = (n-b) \bmod n = n-b$

$(b+(-b)) \bmod n = (b+n-b) \bmod n = (0+n) \bmod n =$

$= n \bmod n = n \bmod n = 0.$

```
>> mb = mod(-b, n)
>> mod(b + mb, n) = 0
```

Let $n = p = 11$: $\mathcal{Z}_p = \{0, 1, 2, \ldots, p-1\}$

Then $\mathcal{Z}_{11} = \{0, 1, 2, 3, \ldots, 10\}$; $+ \bmod 11$; $- \bmod 11$; $* \bmod 11$; $/ \bmod 11$

$\mathcal{Z}_p^* = \{1, 2, 3, \ldots, p-1\}$

Let we have any set ***G*** consisting of the elements of any nature, i.e. ***G***={***a***, ***b***, ***c***, …, ***z***, …}.

1. ***Definition***. *A set **G** is an commutative 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***.
4. *Any element **a** in **G** has its inverse* a^{-1} *with respect to • operation such that* $a \bullet a^{-1} = a^{-1} \bullet a = e$ when ***e*** is neutral el.

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 $\mathcal{Z}_p^* = \{1, 2, 3, \ldots, p-1\}$ where operation is multiplication $\bmod p$ is a multiplicative cyclic group.

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

The set G is algebraic group if 1 binary operation * is defined and

1. G is closed with respect to this operation.
2. There exixts neutral element 1 (some times denoted by e).

3. For all z in G there exixts inverse element z^{-1} such that $z*z^{-1} = (z/z) = 1$.
4. G is cyclic if there exists some element g named as a generator, generating all elements of G.

Multiplication Tab. Z_{11}* mod 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

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

$12 : 11 = 1$, remainder 1

$4 \cdot 3 \bmod 11 = 12 \bmod 11 = 1$

$4 \cdot 4^{-1} \bmod 11 = (4/4) = 1$

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

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

$5^{-1} \bmod 11 = 9$

$45 : 11 = 4$, remainder 1

Power Tab. Z_{11}* mod 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

$\mathcal{I}_{11}^* = \{1, 2, 3, \ldots, 10\}$

The set of numbers that are generating all the numbers in the set $\mathcal{I}_{11}^*$ is named as a set of generator $\Gamma_{11} = \{2, 6, 7, 8\}$

~40% of $\mathcal{I}_p^*$

The cardinality of the set is the number of its elements.

Let G be a finite group with $\text{card}(G) = |G| = N$.

Def. 1. The element g is a generator if g^i, $i = 0, 1, 2, N-1$, generates all N elements of G.

Def. 2. The group G which can be generated by generator

g is a cyclic group and is denoted by $\langle g \rangle = G$.

Cyclic Group: $\mathbf{Z}_p^* = \{1, 2, 3, \ldots, p-1\}$; $\bullet_{\mathbf{mod}\ p}$, $:_{\mathbf{mod}\ p}$.

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

If $p = 11$, then
$q = (11-1)/2 = 5$
p, q are primes

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:
$DEF_{g,p}(x) = g^x \bmod p = a$.

› Documents › 100 MOKYMAS 1 DEF v-4.pptx

Till this place

Discrete Exponent Function DEF :

$DEF_{P,g}(x) = g^x \bmod p = a$.

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

$x \in \mathcal{Z}_{10}$

$\mathcal{Z}_{11}^* = \{1, 2, 3, \ldots, 10\}$
$\mathcal{Z}_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$
$DEF : \mathcal{Z}_{10} \to \mathcal{Z}_{11}^*$
$DEF_2(x) = 7^x \bmod 11 = a \in \mathcal{Z}_{11}^*$

Discrete Exponent Function - DEF (1/14)

The Discrete Exponent Function (**DEF**) used in cryptography firstly was introduced in the cyclic multiplicative group $Z_p^* = \{1, 2, 3, \ldots, p\text{-}1\}$, with binary multiplication operation *** mod** p, where p is prime number. Further the generalizations were made especially in *Elliptic Curve Groups* laying a foundation of *Elliptic Curve CryptoSystems* (ECCS) in general and in *Elliptic Curve Digital Signature Algorithm* (ECDSA) in particular.

Let z be any number in $\boldsymbol{Z_p^*}$ then **DEF** is defined in the following way:

$$\mathbf{DEF}_{z,p}(x) = z^x \bmod p = a;$$

DEF argument x is associated with the private key – **PrK** (or other secret parameters) and therefore we will label it in red and value a is associated with public key – **PuK** (or other secret parameters) and therefore we will label it in green.

In order to ensure the security of cryptographic protocols, a large prime number p is chosen.
This prime number has a length of 2048 bits, which means it is represented in decimal as being on the order of 2^{2048}, or approximately $p \sim 2^{2048} \sim 10^{700}$.

In our modeling with Octave, we will use p of length having only 28 bits for convenience. We will deal also with a strong prime numbers.

Discrete Exponent Function (12/14)

Let as above p=11 and is strong prime and generator we choose $g = 7$ from the set Γ={2, 6, 7, 8}.
Public Parameters are **PP**=(11,7), Then $\mathbf{DEF}_g(x) = \mathbf{DEF}_7(x)$ is defined in the following way:

$$\mathbf{DEF}_7(x) = 7^x \bmod 11 = a;$$

$\mathbf{DEF}_7(x)$ provides the following 1-to-1 mapping, displayed in the table below.

x	0	1	2	3	4	5	6	7	8	9	*10*	*11*	*12*	*13*	*14*
$7^x \bmod p = a$	1	7	5	2	3	10	4	6	9	8	*1*	*7*	*5*	*2*	*3*

You can see that a values are repeating when x = 10, 11, 12, 13, 14, etc. since exponents are reduced **mod** 10 due to *Fermat little theorem.*

The illustration why 7^x **mod** p values are repeating when x = 10, 11, 12, 13, 14, etc. is presented in computations below:
10 mod 10 = 0; 710 = 70 = 1 mod 11 = 1.
11 mod 10 = 1; 711 = 71 = 7 mod 11 = 7.
12 mod 10 = 2; 712 = 72 = 49 mod 11 = 5.
13 mod 10 = 3; 713 = 73 = 343 mod 11 = 2.
14 mod 10 = 4; 714 = 74 = 2401 mod 11 = 3.
etc.

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

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

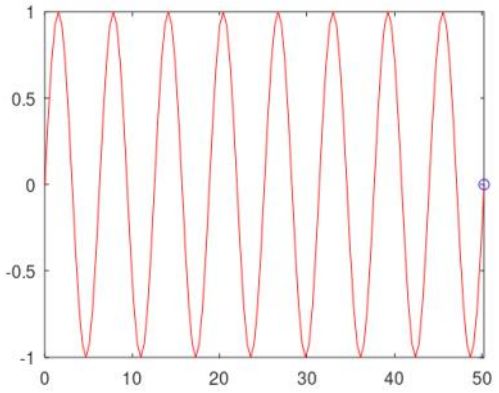
Discrete Exponent Function (13/14)

For illustration of 1-to-1 mapping of $\mathbf{DEF}_7(x)$ we perform the following step-by-step computations.

	$x \in Z_{10}$		$a \in Z_{11}^*$
$7^0 = 1$ **mod** 11	**0**	→	**1**
$7^1 = 7$ **mod** 11	**1**	→	**2**
$7^2 = 5$ **mod** 11	**2**	→	**3**
$7^3 = 2$ **mod** 11	**3**	→	**4**
$7^4 = 3$ **mod** 11	**4**	→	**5**
$7^5 = 10$ **mod** 11	**5**	→	**6**
$7^6 = 4$ **mod** 11	**6**	→	**7**
$7^7 = 6$ **mod** 11	**7**	→	**8**
$7^8 = 9$ **mod** 11	**8**	→	**9**
$7^9 = 8$ **mod** 11	**9**	→	**10**

It is seen that one value of x is mapped to one value of a.

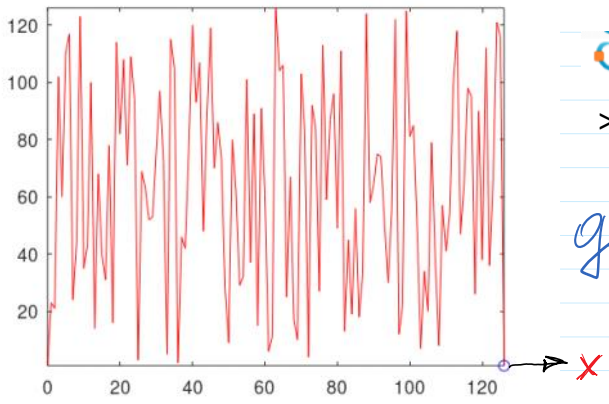
```
>> pi
ans = 3.1416
>> xrange=16*pi
xrange = 50.265
>> step=xrange/128
step = 0.3927
>> x=0:step:xrange;
>> y=sin(x);
>> comet(x,y)
```



p128sin.m

>> p128sin

```
>> p=127
p = 127
>> g = 23
g = 23
>> x=0:p-1;
>> a=mod_expv(g,x,p)
>> comet(x,a)
```



p128def.m

>> p128def

$g^x \bmod p = a$

Discrete Exponent Function (6/14)

Example 1: Let for given integers u, x and h in Z_{p-1} we compute exponent s of generator g by the expression

$$s = u + xh.$$

Then

$$g^s \bmod p = g^{s \bmod (p-1)} \bmod p.$$

Therefore, s must be computed **mod** (p-1) in advance, to save a multiplication operations and to avoid mistakes, i.e.

$$s = u + xh \bmod (p-1).$$

***Example** 2*: Exponent s computation including subtraction by xr **mod** (p-1) and division by i in Z_{p-1} when gcd(i, p-1) = 1.

$$s = (h - xr)i^{-1} \bmod (p-1).$$

Firstly $d = xr$ **mod** (p-1) is computed:
Secondly $-d = -xr$ **mod** (p-1) = (p-1-d) is found.
Thirdly i^{-1} **mod** (p-1) is found.
And finally exponent $s = (h + (p-1-d))i^{-1}$ **mod** (p-1) is computed.

How to ***compute*** i^{-1} **mod** (p-1) when i^{-1} is random generated number:

```
>> i=randi(28)
i = 18
>> i=randi(2^28)
i = 2.0121e+08
>> i=int64(randi(2^28))
i = 146637983
```

```
>> p=genstrongprime(28)
p = 165817343
>> i_m1=mulinv(i,p-1)
i_m1 = 77655747
>> mod(i*i_m1,p-1)
ans = 1
>> gcd(i,p-1)
```

```
>> i=int64(randi(2^28))
i = 118010940
>> i_m1=mulinv(i,p-1)
i_m1 = Inverse element does not exist
>> gcd(i,p-1)
ans = 2
```

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

If p is **strong prime** then p=2q + 1.
Then q = (p-1)/2 is prime as well.
If p = 11, then q = 5.
$G_q = G_5 = \{1, 3, 4, 5, 9\}$.
$|G_q| = q$. $|G5| = 5$.

$3^2 \bmod 11 \neq 1$ & $3^5 \bmod 11 = 1$.
$4^2 \bmod 11 \neq 1$ & $4^5 \bmod 11 = 1$.
$5^2 \bmod 11 \neq 1$ & $5^5 \bmod 11 = 1$.

$9^2 \bmod 11 \neq 1$ & $9^5 \bmod 11 = 1$.

Discrete Exponent Function (10/14)

Notice that there are elements satisfying the following different relations, for example:

$$3^5 = 1 \bmod 11 \text{ and } 3^2 \neq 1 \bmod 11.$$

The set of such elements forms a subgroup of prime order q = 5 if we add to these elements the *neutral group element* 1.

This subgroup has a great importance in cryptography we denote by

$G_5 = \{1, 3, 4, 5, 9\}$.

The multiplication table of G_5 elements extracted from multiplication table of Z_{11}^* is presented below.

Multiplication tab. mod 11	***G*5**				
*	**1**	**3**	**4**	**5**	**9**
1	1	3	4	5	9
3	3	9	1	4	5
4	4	1	5	9	3
5	5	4	9	3	1
9	9	5	3	1	4

Values of inverse elements in G_5

$1^{-1} = 1 \bmod 11$
$3^{-1} = 4 \bmod 11$
$4^{-1} = 3 \bmod 11$
$5^{-1} = 9 \bmod 11$
$9^{-1} = 5 \bmod 11$

Exponent tab. mod 11	***G*5**					
^	**0**	**1**	**2**	**3**	**4**	**5**
1	1	1	1	1	1	1
3	1	3	9	5	4	1
4	1	4	5	9	3	1
5	1	5	3	4	9	1
9	1	9	4	3	5	1

In general, if p is **strong prime** then $p=2q + 1$, and then $q = (p-1)/2$ is prime as well.
Then subgroup G_q consist of elements g' satisfying relation $(g')^q = 1$, i.e. they are of order q.
Subgroup G_q consist of q elements which is prime number.

All elements g' are the generators.
Then g'= is a generator in G_q if and only if (**iff**):
$(g')^2 \bmod 11 \neq 1$ & $(g')^5 \bmod 11 = 1$.

$$\mathrm{DEF}_{g',p}(x) = (g')^x \bmod q \bmod p = a.$$

To find the subgroup G_q is a difficult problem, in general.

Let p is any prime of order $2^{2048} \sim 2^{700}$.
In Digital Signature Algorithm (DSA) standard this subgroup is presented by prime number q as a Public Parameter.
According to Lagrange theorem in Group theory, q must divide the number p-1.
Then expressions in exponents are computed **mod** q.