$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2 \ldots\}$$

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

$\mathbb{Z}$ – ring of integers

1. Closure $+, -, \cdot$
2. Associativity $\forall a, b, c \in \mathbb{Z} \rightarrow (a+b)+c = a+(b+c)$
$(a \cdot b) \cdot c = a \cdot (b \cdot c)$

3. „0" additively neutral element.
$\forall a \in \mathbb{Z}: \quad a + 0 = 0 + a = a$

4. $\forall a \in \mathbb{Z} \rightarrow \exists! \ -a \in \mathbb{Z}: \quad a + (-a) = (-a) + a = 0$
$-a$ is an additively inverse element.

5. „1" is a multiplicatively neutral element
$\forall a \in \mathbb{Z}: \quad a \cdot 1 = 1 \cdot a = a$

6! Not all elements have multiplicatively inverse elem.
such that $a \cdot a^{-1} = a^{-1} \cdot a = 1$ except element 1.

7. Distribution property
$\forall a, b, c \in \mathbb{Z} \rightarrow a \cdot (b + c) = a \cdot b + a \cdot c$

Algorithm in $\mathbb{Z}$:

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

$\gcd(6, 15) = 3 \qquad \gcd(10, 15) = 5$

$\gcd(8, 15) = 1$

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

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

Operation modulo n: mod n.

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

$137 = 12 \cdot 11 + 5$

$$\begin{array}{l} 137 : 11 = 12 \\ \underline{11} \\ 27 \\ 22 \end{array}$$

$137 = 12 \cdot 11 + 5$

11
27
22
5
12

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

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

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

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

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

+	e	o
e	e	o
o	o	e

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

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

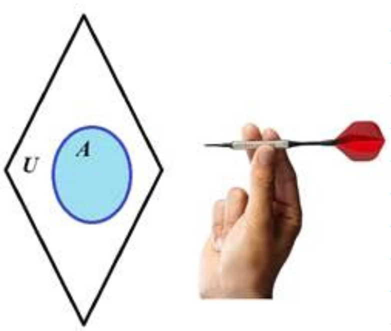
$\oplus$ XOR
Exclusive OR

•	e	o
e	e	e
o	e	o

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

&	0	1
0	0	0
1	0	1

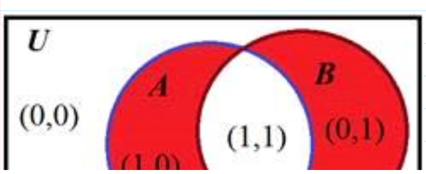
& AND
Conjunction



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.

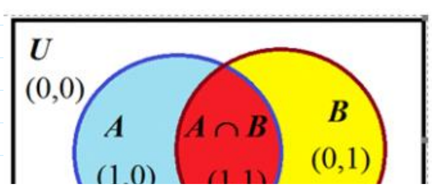
For this single variable b_A the negation (inverse) operation ` is defined:
$b^{\neg}_A$ =0 if b_A=1,
$b^{\neg}_A$ =1 if b_A=0.
Bollean operations are named also as Boolean functions.
Since negation operation/function is performed with the singe variable it is called a unary operation.

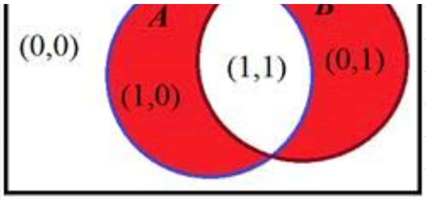
There are 16 Boolean functions defined for 2 variables and called binary functions.
Two of them XOR and AND are illustrated below.



A	B	$A \oplus B$
0	0	0
1	0	1
0	1	1
1	1	0

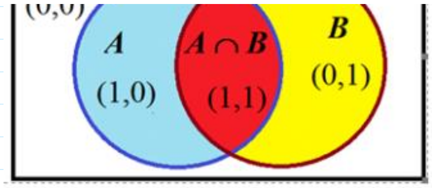
A	B	A & B
0	0	0
1	0	0
0	1	0
1	1	1





1	0	1
0	1	1
1	1	0

1	0	0
0	1	0
1	1	1



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

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

$\langle \mathcal{Z}, +, -, * \rangle$; $\langle \mathcal{Z}_2, \oplus, \& \rangle$

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

$a - a = a \oplus a = 0$; $a \oplus b \oplus a = b \oplus 0 = b$.

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

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

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

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

$$\begin{array}{r|l} 9 & 3 \\ -9 & 3 \\ \hline 0 & \end{array} \qquad \begin{array}{r|l} 7 & 3 \\ -6 & 2 \\ \hline 1 & \end{array} \qquad \begin{array}{r|l} 11 & 3 \\ -9 & 3 \\ \hline 2 & \end{array}$$

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

$\mathcal{Z}_n$ arithmetic $(n < \infty)$: $\mathcal{Z} \bmod n = \mathcal{Z}_n = \{\underset{n}{\overset{\parallel}{0}}, 1, 2, \ldots, n-1\}$

$$\begin{array}{r|l} n & n \\ -n & 1 \\ \hline 0 & \end{array}$$

$\mathcal{Z}_n$ is a ring with operations $+ \bmod n$ or $\cdot \bmod n$

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

$a \; \cdot \bmod n \; b = d \in \mathcal{Z}_n$

Inverse operat.

$- \bmod n$ $\quad$ $/ \bmod n$

$a + b = c \bmod n$

$a \cdot b = d \bmod n$

Operation properties:

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

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

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

$$\begin{array}{r|l} n & n \\ -n & 1 \\ \hline 0 & \end{array}$$

$0 \equiv n \bmod n$

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

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

$(b + (-b)) \bmod n = (\cancel{b} + n - \cancel{b}) \bmod n = (0 + n) \bmod n = n \bmod n = 0.$

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

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

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

```
>> p=11
p = 11
>> a=5
a = 5
>> b=9
b = 9
>> aadb=a+b
aadb = 14
>> aadbp=mod(a+b,p)
aadbp = 3
>> amubp=mod(a*b,p)
amubp = 1
>> a=23
a = 23
>> b=16
```

Number expressed by 4 bits is

$1111 = 1\cdot 2^3 + 1\cdot 2^2 + 1\cdot 2^1 + 1\cdot 2^0 = 15 = 2^4 - 1$

```
>> n=2^28-1
n = 2.6844e+08
>> n=int64(2^28-1)
n = 268 435 455
```

$2^{28} - 1$

$\mathbb{Z}_p^* = \{1, 2, 3, ..., p-1\}$

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* $a•a^{-1}= a^{-1}•a=e$ 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 $\mathbb{Z}_p^* = \{1, 2, 3, ..., p-1\}$ where operation is multiplication mod p is a multiplicative group.

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

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

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

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

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

$\Downarrow$

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

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

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

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

Discrete Exponent Function DEF:

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

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

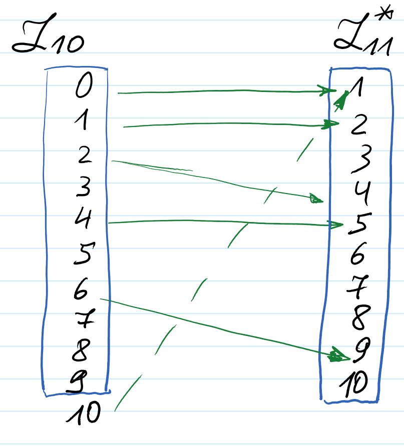
Power Tab. Z_{11}*											
^	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
1	1	1	1	1	1	1	1	1	1	1	1
2	1	2	4	8	5	10	9	7	3	6	1
3	1	3	9	5	4	1	3	9	5	4	1
4	1	4	5	9	3	1	4	5	9	3	1
5	1	5	3	4	9	1	5	3	4	9	1
6	1	6	3	7	9	10	5	8	4	2	1
7	1	7	5	2	3	10	4	6	9	8	1
8	1	8	9	6	4	10	3	2	5	7	1
9	1	9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

$\mathbb{Z}_{11}^* = \{1, 2, 3, \dots, 10\}$

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

$DEF: \mathbb{Z}_{10} \to \mathbb{Z}_{11}^*$

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



Till this place

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

$Card(\mathbb{Z}_{11}^*) = |\mathbb{Z}_{11}| = 10$

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.

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

The set of numbers that are generating all the numbers in the set $\mathbb{Z}_{11}^*$ is named as a set of generator $\Gamma_{11} = \{2, 6, 7, 8\}$
$\sim 40\%$ of $\mathbb{Z}_p^*$

Let G be a finite group with $Card(G) = |G| = N$.
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: $\boldsymbol{Z_p}^* = \{1, 2, 3, \ldots, \boldsymbol{p}-1\}$; $\bullet_{\bmod p}$, $:_{\bmod p}$.

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

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

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

T2. Fermat (little)Theorem. If $\boldsymbol{p}$ is prime, then [Sakalauskas, at al.]

$z \in \mathbb{Z}_p^*$
z^{p-1} ... $z^0 = 1 \bmod p$

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

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

$z \in \mathbb{Z}_p^*$

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

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

$\boxed{p-1 \equiv 0 \bmod p}$

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

Inverse elements in the Group of integers <$\mathbf{Z_p^*}$, **• 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)

$z \in \mathbb{Z}_p^*$: to find z^{-1} such that $z \cdot z^{-1} = z^{-1} * z = 1 \bmod p$

$z^{p-1} = 1 \bmod p \;/ \cdot z^{-1} \Rightarrow z^{p-1} \cdot z^{-1} = z^{-1} \bmod p \Rightarrow$

$\Rightarrow z^{-1} = z^{p-1} \cdot z^{-1} \bmod p \Rightarrow z^{-1} = z^{p-2} \bmod p$

$$z^{-1} = z^{p-2} \bmod p$$

Operations in exponents.

$$\left.\begin{aligned} a^r \cdot a^s \bmod p &= a^{(r+s) \bmod (p-1)} \bmod p \\ (a^r)^s \bmod p &= a^{(r \cdot s) \bmod (p-1)} \bmod p \end{aligned}\right\} \text{According to Fermat th. we have:}$$

$$\left.\begin{aligned} z^0 &= 1 \bmod p \\ z^{p-1} &= 1 \bmod p \end{aligned}\right\} \Rightarrow 0 \equiv p-1 \text{ in exponents } 0 \equiv p-1 \bmod (p-1)$$

Let we need to compute expression: $g^{s \bmod (p-1)} \bmod p$

where s is in exponent of the generator g,

when $s = (i + x \cdot h) \bmod (p-1)$; $r = g^i \bmod p$.

$\sigma = (r, s)$

$$g^{s \bmod (p-1)} \bmod p = g^{(i + x \cdot h) \bmod (p-1)} \bmod p = g^i \cdot (g^x)^h = r \cdot a^h \bmod p.$$

Till this place

Discrete exponent function :

$a = g^{x} \bmod p \; ; \; p \sim 2^{\underbrace{2048}} \approx 10^{700}$

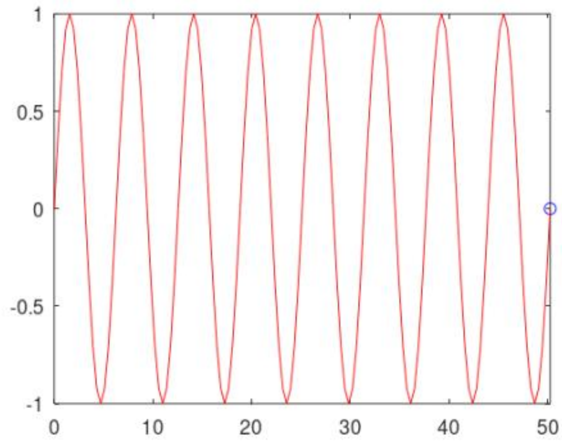
$>> a = \text{mod\_exp}(g, x, p)$

```
>> mod_exp(2,3,7)
ans = 1
```

We will deal with integers of 28 bits

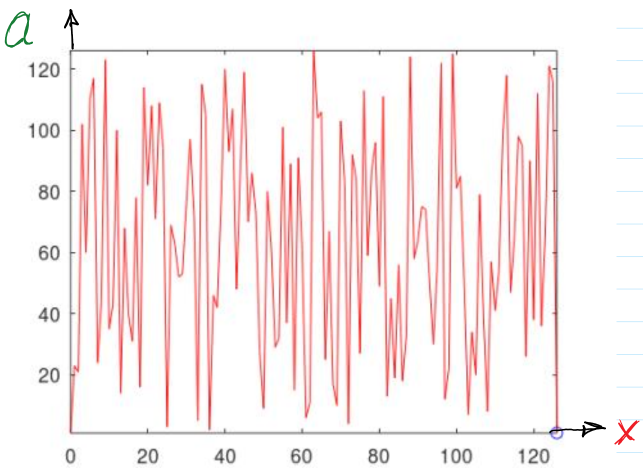
$n \sim 2^{28} - 1$

```
>> 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)
```




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

$g^{x} \bmod p = a$



OWF

One-way-functions : Discrete Exponent Function (DEF) is a conjectured (OWF)

1) It is easy to compute $a = g^x \bmod p$, when x, g, p are given.

2) It is infeasible to find any x satisfying the condition $a = g^x \bmod p$ when a, g, p are given.

Yao theorem: if pseudo random numbers generators exist $\Leftrightarrow$ OWFs exist & vise versa!