Viskas apie pratybas pateikta nuorodoje:
https://docs.google.com/document/d/1__av8t07do9s-7Wtc8EvSi_CVhIZWZ7oFPwN4F66CRg/edit?usp=drivesdk

Operation modulo n : mod n.

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

$137 = 12 \cdot 11 + 5$

$$\begin{array}{r|l} 137 & 11 \\ -11 & 12 \\ \hline 27 & \\ -22 & \\ \hline 5 & \end{array} \qquad \begin{array}{r|l} 4 & 2 \\ -4 & 2 \\ \hline 0 & \end{array}$$

$2 \bmod 2 = 0$

$4 \bmod 2 = 0$

$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, \dots\}$

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

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

$$\begin{array}{r|l} 5 & 2 \\ -4 & 2 \\ \hline 1 & \end{array}$$

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

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

$\mathbb{Z}_2$ arithmetics : $< \mathbb{Z}_2, \overset{XOR}{\oplus}, \overset{AND}{\&} >$

+	e	o
e	e	o
o	o	e

$\xrightarrow[o \equiv 1]{e \equiv 0}$

⊕	0	1
0	0	1
1	1	0

⊕ XOR
Exclusive OR

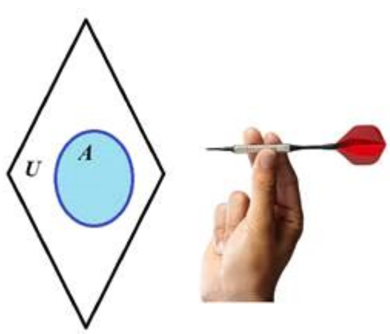
$1 \oplus 1 = 2 \bmod 2 = 0$

•	e	o
e	e	e
o	e	o

$\xrightarrow[o \equiv 1]{e \equiv 0}$

&	0	1
0	0	0
1	0	1

& AND
Conjunction



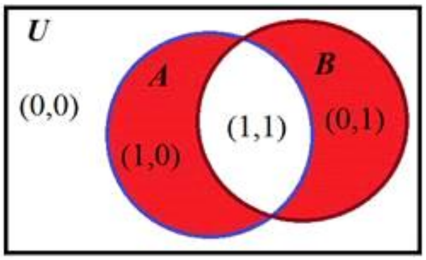
XOR and AND logical operations in Boolean algebra can be illustrated by dartboard game.
Single Boolean variable can be represented by the set of 2 values {0,1} or {Yes,No} or {True,False}.
Let ***U*** is some universal set containing all other sets (we do not takke into account paradoxes related with ***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.

Nebūtina

For this single variable b_A the negation (inverse) operation ` is defined:
b_A`=0 if b_A=1,
b_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.

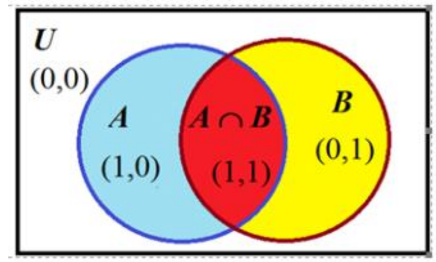
$\bar{b}_A = 1$ if $b_A = 0$.
Bollean operations are named also as Boolean functions.
Since negation operation/function is performed with the singe variable it is called a unary operation.

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



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

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

$n=3: \quad \mathbb{Z} \bmod 3 = \mathbb{Z}_3 = \{0,1,2\}$

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

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

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

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

$9 : 3 = 3$, 9, remainder 0 $\quad 9 \bmod 3 = 0$

$7 : 3 = 2$, 6, remainder 1 $\quad 7 \bmod 3 = 1$

$11 : 3 = 3$, 9, remainder 2 $\quad 11 \bmod 3 = 2$

$\mathbb{Z}_n$ arithmetic $(n<\infty)$: $\mathbb{Z} \bmod n = \mathbb{Z}_n = \{\underset{n}{\overset{\equiv}{0}}, 1, 2, \ldots, n-1\}$ $\quad n : n = 1$, n, remainder 0

Let $n = p$ when p is prime; e.g. $p = 3, 5, 7, 11, \ldots$

Let $p = 11$, Then $\mathbb{Z}_p = \{0, 1, 2, 3, \ldots, 10\}$

```
>> p=11
p = 11
>> isprime(p)
ans = 1

>> a=5
a = 5
>> b=9
b = 9
>> aadb=a+b
```

Number expressed by 4 bits is

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

We will use arithetic of integers having 28 bits
Our arithmetic operations with Octave will be 64 bits integers without sign.

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

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

$Z_p = \{0, 1, 2, 3, \dots, p-1\}$. Let $p=11$ – is prime
$Z \bmod 11 = \{0, 1, 2, 3, \dots, 10\} = Z_{11}$ $p-1 = 11-1 = 10$.
In cryptography the set $Z_p^* = \{1, 2, 3, \dots, p-1\}$ is used instead Z_{11}.

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

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

$12 : 11 = 1$, $12 - 11 = 1$

$4 \cdot 3 \bmod 11 = 12 \bmod 11 = 1$
$4 \cdot 4^{-1} \bmod 11 = (4/4) = 1$
$\Downarrow$
$4^{-1} = 3 \bmod 11$

$5 \cdot 9 = 45 \bmod 11 = 1$
$5^{-1} = 9$

$45 : 11 = 4$, $45 - 44 = 1$

$4 : 4 = 4/4 = \underline{4 * 4^{-1}} = 1$; $4^{-1} = 1/4$
$4 * 4^{-1} = \frac{4}{4} = 1$

>> a=5;
>> b=9;
>> ab=mod(a*b,p)
ab = 1
>> b_m1=mulinv(b,p)
b_m1 = 5

$2^2 = 4$, ... $2^{13} = 8192$
$g^x \bmod p = a$; p – is prime.
g – is a generator in $Z_p^* = \{1, 2, 3, \dots, p-1\}$; $g \in Z_p^*$.

mod p DEF
Discret Exponent Func.

>> x=int64(randi(10)) % random integer x generation with upper bound 10
x = 4
>> g=2
g = 2
>> a=mod_exp(g,x,p) % $a = g^x \bmod p$
a = 5
>> g_x=g^x % g^x
g_x = 16
>> aa=mod(g_x,p) % $aa = a^x \bmod p$

>> x=int64(randi(2^28-1))
x = 150999714
>> xb=dec2bin(x)
xb = 1001 0000 0000 0001 0010 1010 0010

```
>> g_x=g^x
g_x = 16
>> aa=mod(g_x,p)
aa = 5
```

% g^x

% $aa = g^x \bmod p$

xb = 1001 0000 0000 0001 0010 1010 0010