

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

$\langle \mathcal{Z}, +, -, \cdot, / \rangle$; \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.

$$\forall a \in \mathcal{Z} : a+0 = 0+a = a$$

4. $\forall a \in \mathcal{Z} \rightarrow \exists! -a \in \mathcal{Z} : a+(-a) = (-a)+a = 0$

$-a$ is an additively inverse element.

5. "1" is a multiplicatively neutral element

$$\forall a \in \mathcal{Z} : a \cdot 1 = 1 \cdot a = a$$

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

$$\forall a, b, c \in \mathcal{Z} \rightarrow a \cdot (b+c) = a \cdot b + a \cdot c$$

Algorithm in \mathcal{Z} :

1. Greatest Common Divider: $\Rightarrow \text{gcd}(a, n)$

$$\text{gcd}(6, 15) = 3$$

$$\text{gcd}(10, 15) = 5$$

$$\text{gcd}(8, 15) = 1$$

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

2. Extended Euklid Algorithm: $\Rightarrow \text{eeuklid}(a, n)$

Operation modulo n : $\text{mod } n$.

Pvz. 1. $137 \text{ mod } 11 = 5$

$$137 = 12 \cdot 11 + 5$$

$$\begin{array}{r} 137 \quad | \quad 11 \\ 11 \quad | \quad 12 \\ \hline 27 \\ 22 \end{array}$$

$$137 = 12 \cdot 11 + 5$$

$$\begin{array}{r} 11 \cdot 12 \\ \underline{27} \\ 22 \\ \underline{5} \end{array}$$

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

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

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

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

\mathcal{L}_2 arithmetics : $\langle \mathcal{L}_2, \overset{\text{XOR}}{\oplus}, \overset{\text{AND}}{\&} \rangle$

+	e	o
e	e	o
o	o	e

$$\begin{array}{l} e \equiv 0 \\ o \equiv 1 \end{array} \rightarrow$$

\oplus	0	1
0	0	1
1	1	0

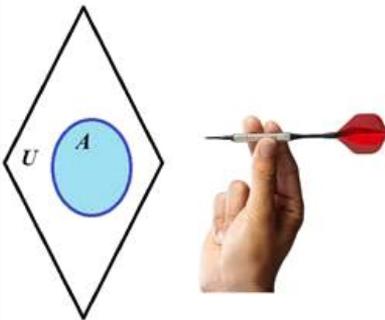
\oplus XOR
Exclusive OR

.	e	o
e	e	e
o	e	o

$$\begin{array}{l} e \equiv 0 \\ o \equiv 1 \end{array} \rightarrow$$

$\&$	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 $\{\text{Yes, No}\}$ or $\{\text{True, False}\}$.

Let U is some universal set containing all other sets (we do not take 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 $\bar{}$ is defined:

$$b_A^{\bar{}} = 0 \text{ if } b_A = 1,$$

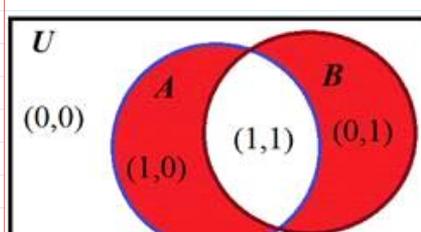
$$b_A^{\bar{}} = 1 \text{ if } b_A = 0.$$

Boolean operations are named also as Boolean functions.

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

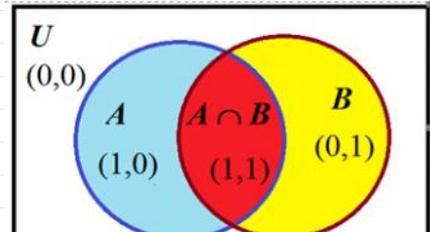
There are 16 Boolean functions defined for 2 variables and called binary functions.

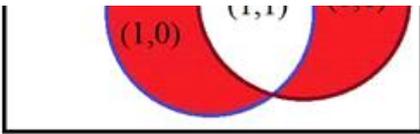
Two of them XOR and AND are illustrated below.



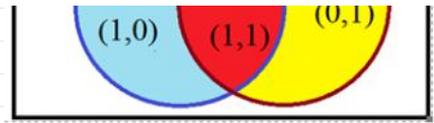
A	B	$A \oplus B$
0	0	0
1	0	1
0	1	1
1	1	0

A	B	$A \& B$
0	0	0
1	0	0
0	1	0
1	1	1





$$1 \ 1 \mid 0 \quad 1 \ 1 \mid 1$$



Venn diagram of $A \oplus B$ operation.

Venn diagram of $A \& B$ operation.

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

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

$$\oplus \text{ - is additively self-inverse: } a - a = a \oplus a = 0; \quad a \oplus b \oplus a = b \oplus 0 = b.$$

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

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

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

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

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

$$\begin{array}{r} 8 \overline{) 3} \\ \underline{6} \\ 2 \end{array} \quad \begin{array}{r} 7 \overline{) 3} \\ \underline{6} \\ 1 \end{array} \quad \begin{array}{r} 12 \overline{) 3} \\ \underline{12} \\ 0 \end{array}$$

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

\mathcal{I}_n is a ring with operations

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

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

$+_{\bmod n}$ or $\cdot_{\bmod n}$

Inverse operat.

$-_{\bmod n}$

$/_{\bmod n}$

$$a + b = c \bmod n$$

$$a \cdot b = d \bmod n$$

Operation properties:

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

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

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

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

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

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

$$\begin{array}{r} - \ n \overline{) n} \\ \underline{-n} \\ 0 \end{array} \quad \begin{array}{r} \ n \overline{) n} \\ \underline{n} \\ 0 \end{array}$$

$$0 \equiv n \bmod n$$

$$\gg mb = \text{mod}(-b, n)$$

$$\gg \text{mod}(b + mb, n) = 0$$

$$\text{Let } n = p = M : \mathcal{Z}_p = \{0, 1, 2, \dots, p-1\}$$

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

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

Let us have any set G consisting of the elements of any nature, i.e. $G = \{a, b, c, \dots, z, \dots\}$.

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

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

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

Discrete Exponent Function - DEF (1/14)

The Discrete Exponent Function (DEF) used in cryptography firstly was introduced in the cyclic multiplicative group $Z_p^* = \{1, 2, 3, \dots, p-1\}$, with binary multiplication operation $* \bmod p$, 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 g be a generator of Z_p^* then DEF is defined in the following way:

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

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 $p \sim 2^{2048}$.

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.

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

$2 \cdot 6 = 12 \pmod{11} = 1$

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

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

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

$5 \cdot 9 = 45 \pmod{11} = 1$

$$\begin{array}{r} 45 \quad | \quad 11 \\ -44 \\ \hline 1 \end{array}$$

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

The set of numbers that are generating all the numbers in the set \mathcal{I}_M^* is named as a set of generator $\Gamma_M = \{2, 6, 7, 8\}$ $\sim 40\%$ of \mathcal{I}_p^*

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

Def. 1. The element g is a generator if $g^i, i = 0, 1, 2, \dots, N-1$, 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: $Z_p^* = \{1, 2, 3, \dots, p-1\}$; $\bullet \bmod p$, $\circ \bmod p$.

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) $g^2 \neq 1 \bmod p$ and $g^q \neq 1 \bmod p$.

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: $g^2 \neq 1 \bmod p$ and $g^q \neq 1 \bmod p$.

The main function used in cryptography is Discrete Exponent Function - DEF:

$$DEF_g(x) = g^x \bmod p = a.$$

> Documents > 100 MOKYMAS

1 DEF v-4.pptx

Discrete Exponent Function DEF :

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

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

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

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

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

$$DEF_2(x) = 7^x \bmod 11 = a \in Z_{11}^*$$

Discrete Exponent Function (12/14)

Let as above $p=11$ and is strong prime and generator we choose $g=7$ from the set $\Gamma=\{2, 6, 7, 8\}$.

Public Parameters are $PP=(11,7)$, Then $DEF_g(x) = DEF_7(x)$ is defined in the following way:

$$DEF_7(x) = 7^x \bmod 11 = a;$$

$DEF_7(x)$ 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 $7^x \bmod p$ values are repeating when $x = 10, 11, 12, 13, 14$, etc. is presented in computations below:

$$10 \bmod 10 = 0; 7^{10} = 7^0 = 1 \bmod 11 = 1.$$

$11 \bmod 10 = 1$; $711 = 71 = 7 \bmod 11 = 7$.
 $12 \bmod 10 = 2$; $712 = 72 = 49 \bmod 11 = 5$.
 $13 \bmod 10 = 3$; $713 = 73 = 343 \bmod 11 = 2$.
 $14 \bmod 10 = 4$; $714 = 74 = 2401 \bmod 11 = 3$.
 etc.

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

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

Discrete Exponent Function (13/14)

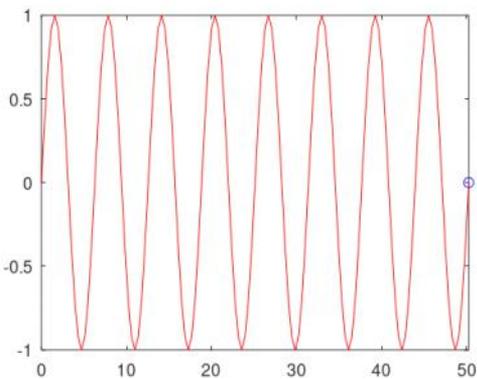
For illustration of 1-to-1 mapping of $DEF_7(x)$ we perform the following step-by-step computations.

	$x \in \mathbb{Z}_{10}$	$a \in \mathbb{Z}_{11}^*$
$7^0 = 1 \bmod 11$	0	1
$7^1 = 7 \bmod 11$	1	2
$7^2 = 5 \bmod 11$	2	3
$7^3 = 2 \bmod 11$	3	4
$7^4 = 3 \bmod 11$	4	5
$7^5 = 10 \bmod 11$	5	6
$7^6 = 4 \bmod 11$	6	7
$7^7 = 6 \bmod 11$	7	8
$7^8 = 9 \bmod 11$	8	9
$7^9 = 8 \bmod 11$	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

