eligijus.sakalauskas@ktu.lt

[2022 will be the year of adjusting to new realities according to The Economist's The World Ahead 2022 (prnewswire.com)](https://www.prnewswire.com/news-releases/2022-will-be-the-year-of-adjusting-to-new-realities-according-to-the-economists-the-world-ahead-2022-301419393.html)

2022 will be the year of adjusting to new realities according to The Economist's The World Ahead 2022

From <https://www.prnewswire.com/news-releases/2022-will-be-the-year-of-adjusting-to-new-realities-according-to-the-economists-the-world-ahead-2022-301419393.html>

https://coinmarketcap.com/

Bitcoin - BTC https://bitcoin.org/en/

Ethereum - ETH https://ethereum.org/

Monero https://www.getmonero.org/

Solidity

Smart Contracts

Cryptology: Information confidentiality, authenticity, integrity and authority (person identification).

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

$< \mathbb{Z}, +, \cdot >$; $\mathbb{Z}$ is closed with respect to $+, \cdot$

$\mathbb{Z}$ - 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 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.

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

$137 \;|\; 11$
$11 \quad\; 12$

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

$137 = 12 \cdot 11 + 5$

$$\begin{array}{r|l} 137 & 11 \\ \hline 11 & 12 \\ \hline 27 & \\ 22 & \\ \hline 5 & \end{array}$$

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

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

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

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

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

+	e	o
e	e	o
o	o	e

$e \equiv 0$, $o \equiv 1$ →

⊕	0	1
0	0	1
1	1	0

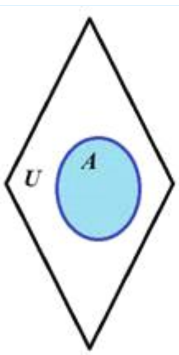
⊕ XOR Exclusive OR

·	e	o
e	e	e
o	e	o

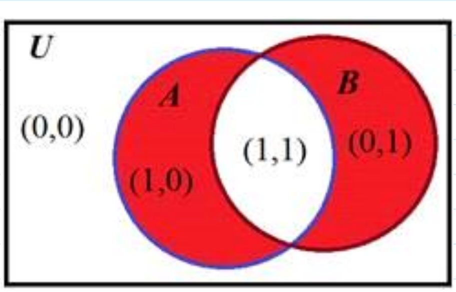
$e \equiv 0$, $o \equiv 1$ →

&	0	1
0	0	0
1	0	1

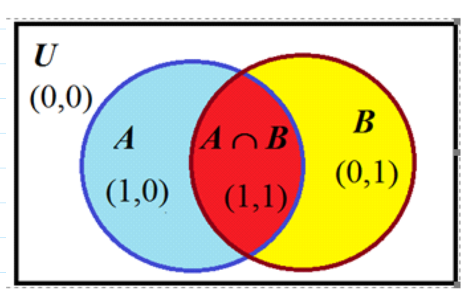
& AND Conjunction $\cap$ And



The simplest dartboard example representing universal set ***U*** with the set ***A*** included inside.
If the target **A** is hit by missile then the outcome is logical **1** and it is **0** otherwise.



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



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

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

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

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

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

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

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

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

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

$a \cdot_{\bmod n} b = d \in \mathbb{Z}_n$

Inverse operat. $-\bmod n$

$a + b = c \bmod n$

$a \cdot b = d \bmod n$

Operation properties:

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

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

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

$0 \equiv n \bmod n$

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

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

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

Additively neutral element to b $\quad -b \bmod n = n - b \quad$ [Octave]

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

$(a^r \cdot a^s) \bmod n = a^{r+s} \bmod n$

$(a^r)^s \bmod n = a^{r \cdot s} \bmod n$

Depending of n the operations $\left.\begin{matrix} r+s \\ r \cdot s \end{matrix}\right\}$ in exponents will be computed differently.

Let $n = p = 11$

Then $\mathbb{Z}_n = \{0, 1, 2, 3, \ldots, 10\}$

```
>> p=11
```

Then $\alpha_n = \{0,1,2,3,\ldots,10\}$

```
>> 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
```

Modular exponent function :

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

```
>> a = mod_exp(g,x,p)
```

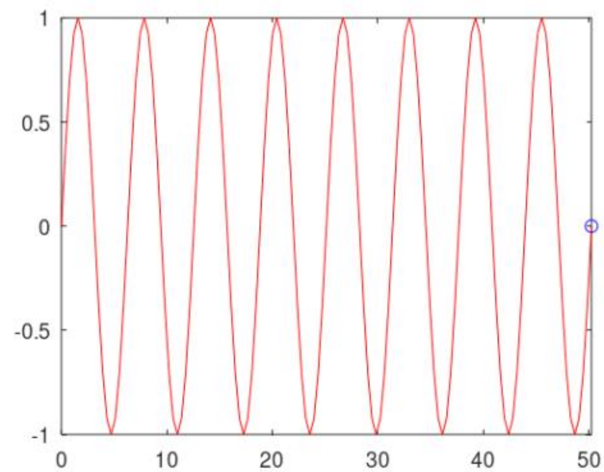
```
>> mod_exp(2,3,7)
ans = 1
```

We will deal with integers of 28 bits

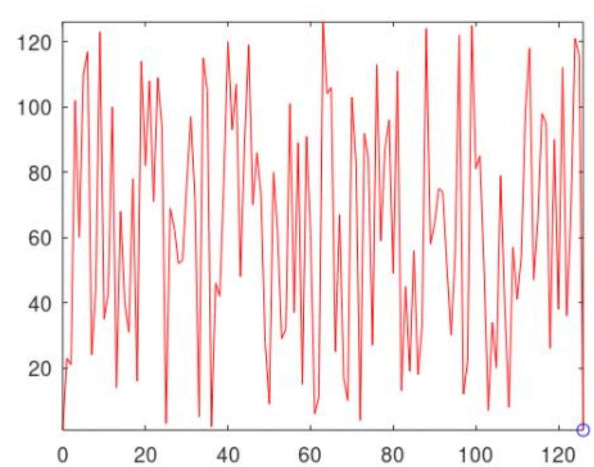
$n \sim 2^{28} - 1$

```
>> n=2^28-1
n = 2.6844e+08
>> n=int64(2^28-1)
n = 268435455
```

```
>> 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)
```



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 $\Rightarrow$ OWFs exist & vise versa!

Till this place

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***.
4. *Any element* ***a*** *in* **G** *has its inverse* $\boldsymbol{a^{-1}}$ *with respect to • operation such that* $\boldsymbol{a \bullet a^{-1} = a^{-1} \bullet a = e}$.

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

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

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

$3 \cdot 10 = 30 \mid 11$
$\quad 22 \quad 2$
$\quad 8$

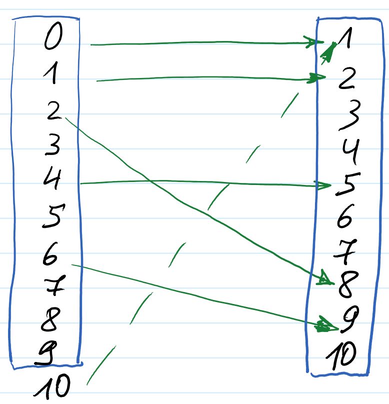
$10 \cdot 10 = 100 \mid 11$
$\quad 99 \quad 9$
$\quad 1$

$4 \cdot 3 \bmod 11 = 12 \bmod 11 = 1$
$4 \cdot 4^{-1} \bmod 11 = \quad = 1$
$\Downarrow$
$4^{-1} = 3 \bmod 11$

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

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

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



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

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.

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

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 $\langle g \rangle = G$.

C.5.3 Finding generators.
We have to look inside $\boldsymbol{Z_P}$* and find a generator. How? $\quad Z_p^* = \{1, 2, 3, \ldots, p-1\}$, $p \sim 2^{2048}$
Even if we have a candidate, how do we test it?
The condition is that $\langle g \rangle = G$ which would take $|G|$ steps to check: $p \sim 2^{2048}$ --> $|G| \sim 2^{2048}$.
In fact, finding a generator given p is in general a hard problem.

We can exploit the particular prime numbers names as **strong primes**.
If p is prime and $p = 2q+1$ with q prime then p is a **strong prime**.
Note that the order of the group $\boldsymbol{Z_P}$* is $p-1 = 2q$, i.e. $|Z_P^*| = 2q$.
Fact C.23. Say $p = 2q+1$ is **strong prime** where $q = (p-1)/2$ is prime, then g in $\boldsymbol{Z_P}$* is a generator of $\boldsymbol{Z_P}$* iff $g^2 \neq 1 \bmod p$ and $g^q \neq 1 \bmod p$.
Testing whether g is a generator is easy given strong prime p.
Now, given $p = 2q+1$, the generator can be found by randomly generation numbers $g < p$ and verifying two relations.The probability to find a generator is ~0.4.

How to fing more generators when **g** one is found?

Fact C.24. If ***g*** is a generator and ***i*** is not divisible by ***q*** and **2** then g^i is a generator as well, i.e.
If ***g*** is a generator and gcd(***i***,***q***)=1 and gcd(***i***,2)=1, then g^i is a generator as well.

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

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

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

Inverse elements in the Group of integers $\langle Z_p^*, \bullet \bmod p \rangle$ can be found using either
Extended Euclidean algorithm or Fermat theorem, or ...

$z \in Z_p^*$: 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.

$$\left.\begin{array}{l} a^r \cdot a^s \bmod p = a^{(r+s) \bmod (p-1)} \bmod p \\ (a^r)^s \bmod p = a^{(r \cdot s) \bmod (p-1)} \bmod p \end{array}\right\}$$

According to Fermat th. we have:

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

Needed example : to comput $s = t + x \cdot h \bmod (p-1)$
when s is in exponent of the generator g :

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