http://crypto.fmf.ktu.lt/telekonf/archyvas/KK%20Blockchain/KK%20BlockChain%202024_P/

$137 \bmod p = 137 \bmod 11 = 6$

$\bmod p$, kai p - pirminis,

$a \cdot b \bmod p = c \in \mathcal{Z}_p = \{0, 1, 2, 3, \ldots, p-1\}$

$11 \bmod 11 = 0$; $22 \bmod = 0$; $23 \bmod 11 = 1$

$\mathcal{Z}_p^* = \{1, 2, 3, \ldots, p-1\}$; $\mathcal{Z}_{11}^* = \{1, 2, 3, \ldots, 10\}$

$137 \mid 11$: -11, 27, -22, 6; 12

$11 \mid 11$: -11, 0; 1

$22 \mid 11$: -22, 0; 2

$23 \mid 11$: -22, 1; 2

$16 \mid 11$: -11, 5; 1

$\mathcal{Z}_{10} = \{0, 1, 2, \ldots, 9\}$

Exponent tab. mod 11 Z_{11}^*	Z_{10}										
^	**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

$2^2 \neq 1 \bmod 11$ & $2^5 \neq 1 \bmod 11$

$6^2 \neq 1 \bmod 11$ & $6^5 \neq 1 \bmod 11$

$7^2 \neq 1 \bmod 11$ & $7^5 \neq 1 \bmod 11$

$8^2 \neq 1 \bmod 11$ & $8^5 \neq 1 \bmod 11$

In cryptography p is very large prime number which length is ~ 2048 bits

$p \sim 2^{2048} \approx 10^{700}$

We will use p having 28 bits length.

$p \sim 2^{28} \approx 2 \cdot 10^6$

In general, it is a hard problem, to find a generator of $\boldsymbol{Z_p^*}$ but using **strong prime** $\boldsymbol{p}$ the generator in $\boldsymbol{Z_p^*}$ can be found by random search satisfying two following conditions: number $\boldsymbol{p}$ must be strong prime.
Number $\boldsymbol{p}$ is strong prime if it is prime and $\boldsymbol{p} = 2*\boldsymbol{q} + 1$, when $\boldsymbol{q}$ - is prime. Then $\boldsymbol{q} = (\boldsymbol{p}-1)/2$.
For example: $\boldsymbol{p} = 11$, then $\boldsymbol{p} = 2*5 + 1 = 11$.

```
>> p=genstrongprime(28)
p = 260 563 559
>> pb=dec2bin(p)
pb = 1111 1000 0111 1110 0010 0110 0111
>> isprime(p)
ans = 1
>> isprime(12)
ans = 0
>> q=(p-1)/2
q = 130281779
>> isprime(q)
ans = 1
```

```
>> g=2
g = 2
>> mod_exp(g,q,p)
ans = 1
>> g=3
g = 3
>> mod_exp(g,q,p)
ans = 1
>> g=4
g = 4
>> mod_exp(g,q,p)
ans = 1
>> g=5
```

ans = 1

```
>> g=5
g = 5
>> mod_exp(g,q,p)
ans = 1
>> g=6
g = 6
>> mod_exp(g,q,p)
ans = 1
>> g=7
g = 7
>> mod_exp(g,q,p)
ans = 260563558
```

Let p is strong prime $p = 2*q + 1$, when q - is prime, then for all $g \in \Gamma$ $g^q \neq 1 \bmod p$; and $g^2 \neq 1 \bmod p$.

For cryptographis system creation needs to define so calle Public Parameters $PP = (p, g)$.
In our case **p = 260 563 559, g = 7**

Discrete Exponent Function (12/14)

Let as above p=11 and is strong prime in $\mathbf{Z}_{11}^*$ ={1, 2, 3, …, 10} 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:

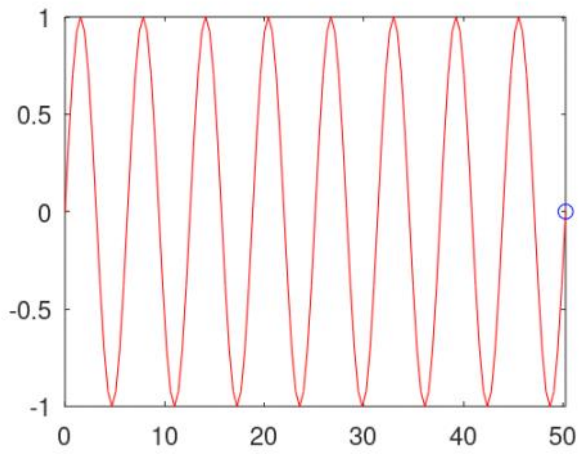
$$\mathbf{DEF}_7(x) = 7^x \bmod 11 = a;$$

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

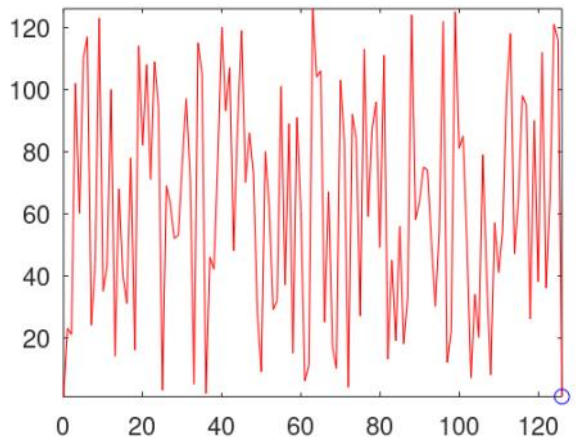
x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$7^x \bmod p = a$	1	7	5	2	3	10	4	6	9	8	1	7	5	2	3

$7 \cdot 7 = 49$, $49 - 44 = 5$, $44 = 11 \cdot 4$

>> p128sin



>> p128def



Private and Public keys generation: $PrK = x$; $PuK = a$;
1) Generate strong prime number P.
2) Find a generator g in the set $\mathcal{I}_p^* = \{1, 2, 3, \ldots, p-1\}$
3) Generate $PrK = x$ using random number generator randi

```
>> x = int64(randi(2^28-1))
```

>> x = int64(randi($2^{28}-1$))

4) compute Puk = a using function

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