```
>> mod(9^2,11)
ans = 4
>>
>> mod_exp(9,2,11)
ans = 4
>> mod(5+9,11)
ans = 3
>> mod(5-9,11)
ans = 7
>> mod(-9,11)
ans = 2
>> mod(5+2,11)
ans = 7
>> mod(11,11)
ans = 0
```

```
n = 15
>> dec2hex(n)
ans = F
>> hex2bin(ans)
ans = 1111
```

Random integers generation.

```
>> r=randi(2^4-1)
r = 8
>> dec2bin(r)
ans = 1000
```

$1000 = 1\cdot 2^3 + 0\cdot 2^2 + 0\cdot 2^1 + 0\cdot 2^0 = 8$

```
>> r28=randi(2^28-1)
r28 = 2.2644e+08
>> r28=int64(randi(2^28-1))
r28 = 105274044
>> r28b=dec2bin(r28)
r28b = 110 0100 0110 0101 1010 1011 1100
>> nmax=2^28-1
nmax = 2.6844e+08
>> nmax=int64(2^28-1)
nmax = 268435455
>> nmaxb=dec2bin(nmax)
nmaxb = 1111 1111 1111 1111 1111 1111 1111
>> nmaxh=bin2hex(nmaxb)
nmaxh = FFFFFFF

nmaxh =    F    F    F    F    F    F    F
nmaxb = 1111 1111 1111 1111 1111 1111 1111
```

```
>> p=genstrongprime(28)
p = 201318479
>> isprime(p)
ans = 1
>> q=(p-1)/2
q = 100659239
>> isprime(q)
ans = 1
```

Cyclic Group: $\boldsymbol{Z_p}^* = \{1, 2, 3, \ldots, \boldsymbol{p}-1\}$; $\bullet_{\text{mod } p}$, $:_{\text{mod } p}$.

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

```
>> p=11;
>> daug_lent(p)
ans =

  1   2   3   4   5   6   7   8   9  10
  2   4   6   8  10   1   3   5   7   9
  3   6   9   1   4   7  10   2   5   8
  4   8   1   5   9   2   6  10   3   7
  5  10   4   9   3   8   2   7   1   6
  6   1   7   2   8   3   9   4  10   5
  7   3  10   6   2   9   5   1   8   4
  8   5   2  10   7   4   1   9   6   3
```

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

```
 6   1   7   2   8   3   9   4  10   5
 7   3  10   6   2   9   5   1   8   4
 8   5   2  10   7   4   1   9   6   3
 9   7   5   3   1  10   8   6   4   2
10   9   8   7   6   5   4   3   2   1
```

```
>> mulinv(8,11)
ans = 7
>> mod(8*7,11)
ans = 1
```

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

```
>> dexp_lent(p)
ans =

  1  2  3  4  5  6  7  8  9 10
  2  4  8  5 10  9  7  3  6  1
  3  9  5  4  1  3  9  5  4  1
  4  5  9  3  1  4  5  9  3  1
  5  3  4  9  1  5  3  4  9  1
  6  3  7  9 10  5  8  4  2  1
  7  5  2  3 10  4  6  9  8  1
  8  9  6  4 10  3  2  5  7  1
  9  4  3  5  1  9  4  3  5  1
 10  1 10  1 10  1 10  1 10  1
```

~40% numbers are generators

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

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

```
>> p=genstrongprime(28)
p = 187086587
>> isprime(p)
ans = 1
>> q=(p-1)/2
q = 93543293
>> isprime(q)
ans = 1
>> g=2;
>> mod_exp(g,2,p)
```

```
>> p=genstrongprime(28)
p = 144668519
>> q=(p-1)/2
q = 72334259
>> g=2;
>> mod_exp(g,q,p)
ans = 1
>> g=7;
>> mod_exp(g,q,p)
ans = 144668518
```

```
>> p=genstrongprime(28)
p = 211504967
>> q=(p-1)/2
q = 105752483
>> g=5
g = 5
>> mod_exp(g,q,p)
ans = 211504966
```

```
>> t=int64(randi(2^28-1))
t = 58435490
>> t_m1=mulinv(t,p)
t_m1 = 194971802
>> mod(t*t_m1,p)
ans = 1
```

ans = 1
>> g=2;
>> mod_exp(g,2,p)
ans = 4
>> mod_exp(g,q,p)
ans = 187086586

>> g=7;
>> mod_exp(g,q,p)
ans = 144668518

ans = 211504966

$a^x \cdot a^y = a^{x+y}$
$(a^x)^y = a^{xy}$

Public parameters used in our course:
>> p = 268 435 019; % 2^28 -1 --> >> int64(2^28-1)
% ans = **268 435 455**

>> g=2;

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

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

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

$z^k \bmod p = z^{k \bmod (p-1)} \bmod p$ $2^{13} \bmod p = 2^{13 \bmod (p-1)} \bmod p$

$DEF_{p,g} : \mathbb{Z}_{p-1} \to \mathbb{Z}_p^*$

>> mod_exp(2,13,pp)
ans = 8
>> e=mod(13,pp-1)
e = 3
>> mod_exp(2,e,pp)
ans = 8

$g^x \cdot g^y \bmod p = g^{(x+y) \bmod (p-1)} \bmod p$

$(g^x)^y \bmod p = g^{xy \bmod (p-1)} \bmod p$

$s = (h - x \cdot r) \cdot i^{-1} \bmod (p-1)$ → $v = g^s \bmod p$

$i^{-1} \bmod (p-1)$ exists iff $\gcd(i, p-1) = 1$.

>> i=int64(randi(2^28-1))
i = 172709820
>> pm1=p-1
pm1 = 211504966
>> i_m1=mulinv(i,p-1)
i_m1 = Inverse element does not exist
>> gcd(i,p-1)
ans = 2

>> i=int64(randi(2^28-1))
i = 218771960
>> i=int64(randi(2^28-1))
i = 123193473
>> gcd(i,p-1)
ans = 1
>> i_m1=mulinv(i,p-1)
i_m1 = 44971013
>> mod(i*i_m1,p-1)
ans = 1

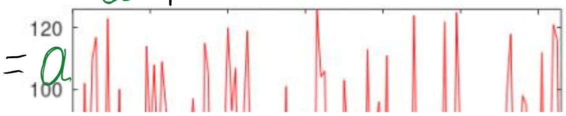
x = 86573915
>> r=int64(randi(2^28-1))
r = 1569199
>> xr=mod(x*r,p-1)
xr = 157637591
>> hmxr=mod(h-xr,p-1)
hmxr = 107115445
>> s=mod(hmxr*i_m1,p-1)
s = 171436121

Till this plaace

>> p=127
p = 127
>> q=(p-1)/2

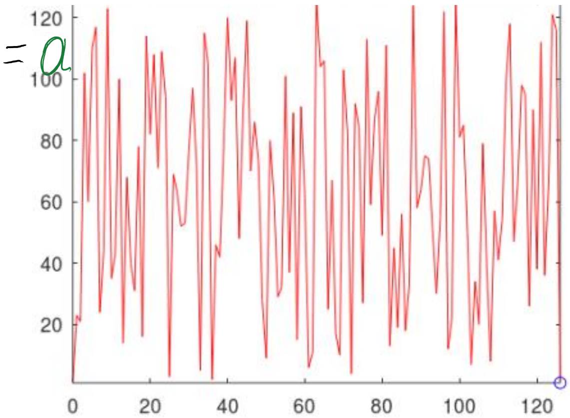
$g^x \bmod p = a$

a ↑



```
>> p=127
p = 127
>> q=(p-1)/2
q = 63
>> g=23
g = 23
>> mod_exp(g,2,p)
ans = 21
>> mod_exp(g,q,p)
ans = 126
```

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



$\rightarrow x$

```
>> p=genstrongprime(28)
p = 144668519
>> g=2;
>> q=(p-1)/2
q = 72334259
>> g=2;
>> mod_exp(g,q,p)
ans = 1
>> g=7;
>> mod_exp(g,q,p)
ans = 144668518
>>
>> a = int64(45951328)
a = 45951328
>> b = int64(170279117)
b = 170279117
>> c = int64(14146341)
c = 14146341
```

compute $t = g^{z} \bmod p$

$z = (a + b*c) \bmod (p-1)$

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

$= g^{(a+b*c) \bmod (p-1)} \bmod p =$

$= g^{a \bmod (p-1)} * g^{b*c \bmod (p-1)} \bmod p$

```
>> bc=mod(b*c,p)
bc = 131688357
>>
>> bc=mod(b*c,p-1)
bc = 3670499
>> z=mod(a+bc,p-1)
z = 49621827
>> g
g = 7
>> t=mod_exp(g,z,p)
t = 135836025
```

```
>> g_a=mod_exp(g,a,p)
g_a = 59261818
>> bc
bc = 3670499
>> g_bc=mod_exp(g,bc,p)
g_bc = 103972682
>>
>> tt=mod(g_a*g_bc,p)
tt = 135836025
```

Parameters **a, b, c** are the same.
Compute $\boldsymbol{t=g^{z}}$ **mod** $\boldsymbol{p}$ and
$\boldsymbol{tt=g^{a} * g^{b*c}}$ **mod p**.

Gilbertas:
z=170167569
t=54811947
g_a=39721727
g_bc=109350828
tt=54811947
Ignas:
t = tt = 54811947