Octave installation

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

>> p=genprime(28)
>> isprime(p)
>> p=genstrongprime(28)
```

$123 \bmod 11 \rightarrow 123 \mid 11$ — 11 — 13 — 11 — 2 — (2)

p- is strong prime if $p = 2 \cdot q + 1$, where q – is prime

p-(strong)prime --> $\boldsymbol{Z_p}=\{0, 1, 2, 3, \ldots, \boldsymbol{p}-1\}$,

$+_{\bmod p}$; $-_{\bmod p}$; $*_{\bmod p}$; $:_{\bmod p}$;

$\boldsymbol{Z_p}^*=\{1, 2, 3, \ldots, \boldsymbol{p}-1\}$.

$*_{\bmod p}$; $:_{\bmod p}$; +; -;

$\boldsymbol{Z_{p-1}}=\{0, 1, 2, \ldots, \boldsymbol{p}-2\}$.

$+_{\bmod p-1}$; $-_{\bmod p-1}$; $*_{\bmod p-1}$; $:_{\bmod p-1}$;

$\Rightarrow |\boldsymbol{Z_p}^*| = |\boldsymbol{Z_{p-1}}|$

p=11 --> $\boldsymbol{Z_{11}}=\{0, 1, 2, 3, \ldots, 10\}$, $Z_{11}^*=\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$.

The set of exp. mod11: $Z_{10}=\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$.

$\Rightarrow |Z_{11}^*| = |Z_{10}|$

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

$2 \cdot 6 = 12 \bmod 11 \rightarrow 12 \mid 11$ — 11 — 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

$2^4 = 16 \bmod 11 \rightarrow 16 \mid 11$ — 11 — 5

$|Z_{11}^*| = 10$ elements

$\Gamma = \{2, 6, 7, 8\}$; $|\Gamma| = 4$

2	1	2	4	8	3	10	9	7	5	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

$\Gamma = \{2, 6, 7, 8\}$; $|\Gamma| = 4$

↑ set of generators in Z_{11}^*

For arbitrary p-prime $|\Gamma| \sim 40\%$ of all elem. in Z_p^*.

C.5.3 Finding generators.

We have to look inside Z_P^* and find a generator. How?

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 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 Z_P^* is a generator of 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.

>> mod_exp(g,2,p); >> mod_exp(g,q,p);

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.

Generation

```
>> g=2
g = 2
>> mod_exp(g,2,p)
ans = 4
>> 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
g = 5
>> mod_exp(g,q,p)
ans = 209192902
```

is a generator of Z_p^*, where p = 209192903

Multiplication Tab	Z10										
*	0	1	2	3	4	5	6	7	8	9	10
0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	0
2	0	2	4	4	8	0	2	4	6	8	0
3	0	3	6	9	2	5	8	1	4	7	0
4	0	4	8	2	6	0	4	8	2	6	0
5	0	5	0	5	0	5	0	5	0	5	0
6	0	6	2	8	4	0	6	2	8	4	0
7	0	7	4	1	8	5	2	9	6	3	0
8	0	8	6	4	2	0	8	6	4	2	0
9	0	9	8	7	6	5	4	3	2	1	0
10	0	0	0	0	0	0	0	0	0	0	0

$Z_{p-1} = Z_{10} = \{0, 1, 2, \dots, 9\}$

Division operation

$a : b \bmod n =$

$= a/b \bmod n =$

$= a \cdot b^{-1} \bmod n.$

multiplicatively inverse number to b mod n:

$b \cdot b^{-1} \bmod n = 1.$

If $\gcd(b, n) = 1 \Rightarrow \exists!\ b^{-1} \in Z_n$ such that

$\gcd(2, 10) = 2$

```
>> gcd(2,10)
ans = 2
>> gcd(6,10)
ans = 2
>> gcd(7,10)
ans = 1
>> mod(7*3,10)
ans = 1
>> mulinv(7,10)
ans = 3
>> mulinv(6,10)
ans = Inverse element does not exist
```

Addition Tab	Z10										
0	0	1	2	3	4	5	6	7	8	9	10
0	0	1	2	3	4	5	6	7	8	9	0

1	1										1
2	2	3	4	5	6	7	8	9	0	1	2
3	3										3
4	4										4
5	5										5
6	6										6
7	7										7
8	8										8
9	9										9
10	0	1	2	3	4	5	6	7	8	9	0

Variables, numbers and transformatios.

Public parameters generatiom

>> p = 268 435 019; % 2^28 --> >> int64(2^28-1)
% ans = **268 435 455**
>> g=2; % testing g=3, g=4, …..