Operation modulo n : mod n.

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

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

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

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

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

+	e	o
e	e	o
o	o	e

$\dfrac{e \equiv 0}{o \equiv 1} \rightarrow$

$\oplus$	0 (B)	1 (B)
A 0	0	1
A 1	1	0

$\oplus$ XOR
Exclusive OR

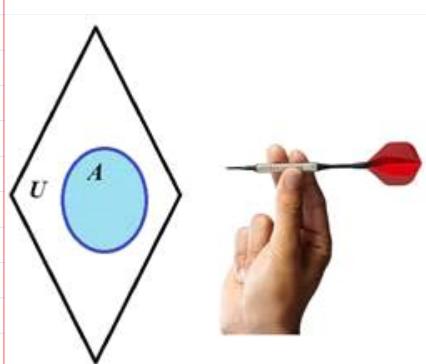
•	e	o
e	e	e
o	e	o

$\dfrac{e \equiv 0}{o \equiv 1} \rightarrow$

&	0	1
0	0	0
1	0	1

& AND
Conjunction

$\cap$ And



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 {Yes,No} or {True,False}.
Let ***U*** is some universal set containing all other sets (we do not takke 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 $\boldsymbol{b_A}$=1 if area ***A*** is hit by missile
$\boldsymbol{b_A}$=0 otherwise.

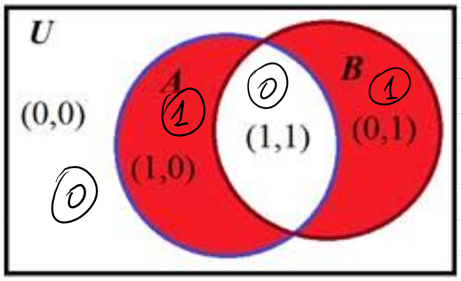
For this single variable b_A the negation operation ` is defined:
$\boldsymbol{b_A}$`=0 if $\boldsymbol{b_A}$=1,
$\boldsymbol{b_A}$`=1 if $\boldsymbol{b_A}$=0.
Bollean operations are named also as Boolean functions.
Since negation operation/function is performed with the singe variable it is called a unary operation.

There are 16 Boolean functions defined for 2 variables and called binaryfunctions.
Two of them XOR and AND are illustrated below.

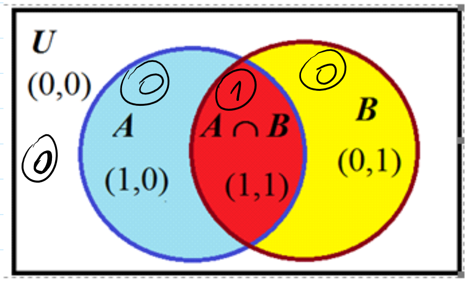
$A \oplus B$

Two of them XOR and AND are illustrated below.

$A \oplus B$



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



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

$\mathbb{Z}_n$ arithmetic $(n<\infty)$: $\mathbb{Z} \bmod n = \mathbb{Z}_n = \{\underset{\substack{\| \\ n}}{0}, 1, 2, \dots, n-1\}$

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

Inverse operat. $- \bmod n$

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

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

$a + b = c \bmod n$

$a \cdot b = d \bmod n$

Operation properties:

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

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

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

$n : n = 1$, $n - n = 0$

$0 \equiv n \bmod n$

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 $-b \bmod n = n - b$ [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 $\mathbb{Z}_n = \{0, 1, 2, 3, \ldots, 10\}$

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 a^{-1} with respect to • operation such that $a \bullet a^{-1} = a^{-1} \bullet a = e$.*
5. If ***a•b*** = ***b•a*** then group ***G*** is commutative group.

Division operation is defined: $a{:}b = a \bullet b^{-1}$

To divide ***a*** by b^{-1} it is necessary to find multiplicatively inverse elemet b^{-1} to ***b*** such that

$b^{-1} \bullet b = b \bullet b^{-1} = 1$.

We will deal with commutative groups.

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. There we present one very important isomorphism example later when consider so called discrete exponent function (DEF).

T1. Theorem. If p is prime, then $\mathbb{Z}_p^* = \{1, 2, 3, \ldots, p-1\}$ where operation is multiplication $*\bmod p$ is a multiplicative group: $\langle \mathbb{Z}_p^*, *\bmod p \rangle$

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

Multiplication Tab. Z₁₁*										
*	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

$3 \cdot 10 = 30 \; | \; 11$

$\quad 22 \quad 2$

$\quad 8$

$10 \cdot 10 = 100 \; | \; 11$

$\quad 99 \quad 9$

$\quad 1$

$$\left.\begin{array}{l} 4 \cdot 3 \bmod 11 = 12 \bmod 11 = 1 \\ 4 \cdot 4^{-1} \bmod 11 = \qquad = 1 \end{array}\right\}$$

$\Downarrow$

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

$4 \cdot 4$ mod ... = ... = 1

$\Downarrow$

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

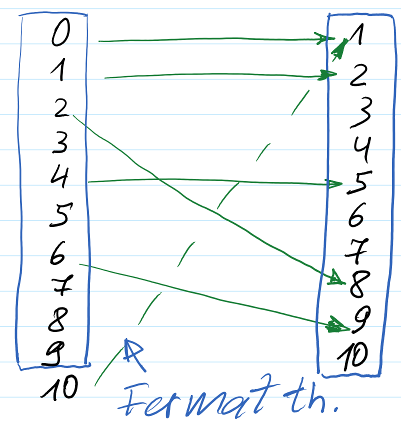
Power Tab. Z_{11}*	$x \in Z_{10}$										
^	0	1	2	3	4	5	6	7	8	9	10
1	1	1	1	1	1	1	1	1	1	1	1
2	1	2	4	8	5	10	9	7	3	6	1
3	1	3	9	5	4	1	3	9	5	4	1
4	1	4	5	9	3	1	4	5	9	3	1
5	1	5	3	4	9	1	5	3	4	9	1
6	1	6	3	7	9	10	5	8	4	2	1
7	1	7	5	2	3	10	4	6	9	8	1
8	1	8	9	6	4	10	3	2	5	7	1
9	1	9	4	3	5	1	9	4	3	5	1
10	1	10	1	10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

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

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

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

$DEF_2(x) = 2^x \bmod p$



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

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. Fermet little th.

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

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

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

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 $\langle g \rangle = G$.

$\langle Z_p^*, * \cancel{\bmod p} \rangle$; $Z_p^* = \{1, 2, 3, \ldots, p-1\}$; $p \sim 2^{2048} \approx 10^{670}$

If g is a generator: $Z_p^* = \{g^e \mid e = 0,1,2,\ldots,p-2\}$

$e \in Z_{p-1} = \{0,1,2,\ldots,p-2\}$

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

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

Using this theorem we can prove that if z=g is a generator then DEF is 1-to-1 mapping:
DEF: $Z_{p-1} \rightarrow Z_p^*$;
DEF(x) = g mod p = a.

Computation of exponent values in Z_p^*

$a^{x\cdot y+z} \bmod p$

$a^{p-1} \bmod p = 1 = a^0 \bmod p \Rightarrow p-1 \equiv 0 \bmod (p-1)$

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

The exponent relation $x\cdot y+z$ can be reduced $\bmod (p-1)$

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

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

```
>> a_xmypz = mod_exp(a, x*y+z, p)
>> xmypz = mod(x*y+z, p-1)
>> a_xmypz = mod_exp(a, xmypz, 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 <***g***> = ***G*** which would take |***G***| steps to check: ***p***~2^{2048} --> |G|~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***=**2*q***+1 with ***q*** prime then ***p*** is a **strong prime**.

Note that the order of the group ***Z_P**** is ***p***-1=2***q***, i.e. |***Z_P****|=2***q***.

Fact C.23. Say ***p***=2***q***+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***=2***q***+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.

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

Inverse elements in the Group of integers <Z_p^*, **• mod p**> can be found using either
Extended Euclidean algorithm or Fermat theorem, or …

$z \in \mathbb{Z}_p^*$: to find z^{-1} such that $z \cdot z^{-1} = z^{-1} * z = 1 \bmod p$

$z^{p-1} = 1 \bmod p \; / \cdot z^{-1} \Rightarrow z^{p-1} \cdot z^{-1} = z^{-1} \bmod p \Rightarrow$

$\Rightarrow z^{-1} = z^{p-1} \cdot z^{-1} \bmod p \Rightarrow z^{-1} = z^{p-2} \bmod p$

$$z^{-1} = z^{p-2} \bmod p$$

```
>> z_m1 = mulinv(z, p)
```

Operations in exponents.

$a^r \cdot a^s \bmod p = a^{(r+s) \bmod (p-1)} \bmod p$ According to Fermat th.

operations in exponents.

$a^r \cdot a^s \bmod p = a^{(r+s) \bmod (p-1)} \bmod p$ } According to Fermat th.
$(a^r)^s \bmod p = a^{(r \cdot s) \bmod (p-1)} \bmod p$ } 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:

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

$$\mathrm{Sign}(PrK, h) = (r, s)$$

Public Parameters generation

$PP = (p, g)$

p - strong prime $\Rightarrow$ it is easy to generate generator g by randomly choosing g values with probability ~ 0.4.

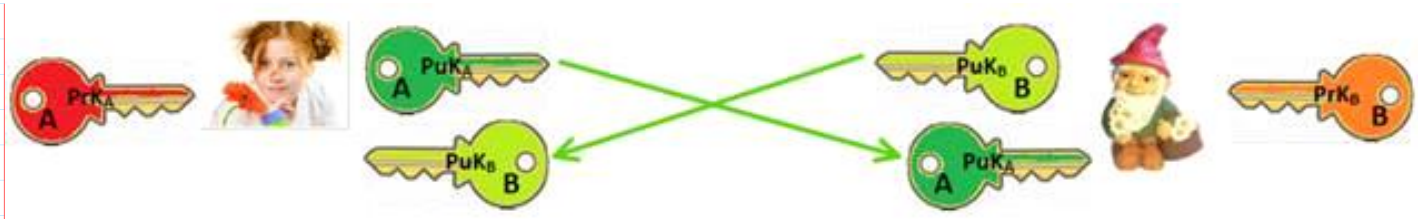
```
>> p =   268 435 019;   % 2^28 --> >> int64(2^28-1)
                        % ans = 268 435 455
>> g=2;                 % testing g=2, g=3, .....
```

Private and Public Keys generation

$PrK = x$ $\qquad$ $PuK = a$

$x \leftarrow \mathrm{randi}(2^{28})$ $\qquad$ $a = g^x \bmod p$

Security of PrK is based on the difficulty of Discrete Logarithm Problem - DLP.
When $p \sim 2^{2048}$, then DLP is infeasible for classical - non-quantum computers.



Google

For Ethereum

Go : 1. PrK & PuK generation   2. Smart contract signing

Solidity

malware

?

Net

Secure PrK, PuK generation & signing

computer

(PrK , PuK) → Flash token

Go Trust (Taiwan)