http://crypto.fmf.ktu.lt/
http://crypto.fmf.ktu.lt/telekonf/archyvas/inf3047%20Kript.Duom.Sauga/

From Aušrys Kilčiauskas to Everyone: 11:18 AM
Lab connection: https://ac.ktu.edu/p170b111
Lab materials and files:
https://drive.google.com/drive/folders/1WG1ToNpQihShfCIF9RIEI7kCTGs2rN0F?usp=sharing

N={0, 1, 2, 3, … }

$\langle N, +, \cdot \rangle$

$2-3=-1 \notin N$

: division operation is not defined in both sets N and Z.

$4:3 = 1,333\ldots \notin N$
$\notin Z$

Z={…, -3, -2, -1,0, 1, 2, 3, … }

$\langle Z, +, \cdot, - \rangle$

$2-3=-1 \in N$

X	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	10
2	0	2	4	6	8	10	12	14	16	18	20
3	0	3	6	9	12	15	18	21	24	27	30
4	0	4	8	12	16	20	24	28	32	36	40
5	0	5	10	15	20	25	30	35	40	45	50
6	0	6	12	18	24	30	36	42	48	54	60
7	0	7	14	21	28	35	42	49	56	63	70
8	0	8	16	24	32	40	48	56	64	72	80
9	0	9	18	27	36	45	54	63	72	81	90
10	0	10	20	30	40	50	60	70	80	90	100

Z_P^*={1, 2, 3, …, p-1} Multiplication operations $*_{\text{mod p}}$

With p - prime number (prime)

$z \in N$, choose ***n***

r - reminder;

$0 \le r < n$

$z = 15;\ n = 13$

$z = 1 \cdot 13 + 2 = 15$

$z = 41;\ n = 13$

$z = 3 \cdot 13 + 2 = 41$

Module (n) operation of any number $z \in N$ is defined

$z \bmod n = r$

It is an unique presentation for given z an n.

When $z = k \cdot n + r$. E. g. 1) $35 \bmod 4 = 3$

$35 = 8 \cdot 4 + 3 = 32 + 3 = 35$

2) $36 \bmod 4 = 0$

$36 = 9 \cdot 4 + 0 = 36 + 0 = 36$

>> mod(35, 4) → ans = 3

Instead of arbitrary n we will use prime number p.

$z = k \cdot p + r \qquad 0 \le r < p$

p - prime ; Let $p = 13$. $Z_{13}^* = \{1, 2, 3, \dots, 12\}$

Multiplication Table $\mathbf{Z_{13}^*}$

1	2	3	4	5	6	7	8	9	10	11	12
2	4	6	8	10	12	1	3	5	7	9	11
3	6	9	12	2	5	8	11	1	4	7	10
4	8	12	3	7	11	2	6	10	1	5	9
5	10	2	7	12	4	9	1	6	11	3	8
6	12	5	11	4	10	3	9	2	8	1	7
7	1	8	2	9	3	10	4	11	5	12	6
8	3	11	6	1	9	4	12	7	2	10	5
9	5	1	10	6	2	11	7	3	12	8	4
10	7	4	1	11	8	5	2	12	9	6	3
11	9	7	5	3	1	12	10	8	6	4	2
12	11	10	9	8	7	6	5	4	3	2	1

$14 \bmod 13 = 1$

Z_{13}^* - is closed under $*_{\bmod 13}$

$14 = 1 \cdot 13 + 1$

1) In the set Z_{13}^* the mult. op. mod 13 is defined

2) Addition operation mod 13 is defined in the set

$Z_{13} = \{0, 1, 2, 3, \dots, 12\}$

A little corrected Table you can find below.

E.g. $8 + 5 = 13 \Rightarrow 13 = 1 \cdot 13 + 0 \Rightarrow r = 0 \Rightarrow 13 \bmod 13 = 0$

3) substraction operation is defined in Z_{13}

$a \in Z_{13} \Rightarrow a - a = 0 \notin Z_{13} \Rightarrow a + (-a) = 0 \pmod{13}$

$5 - 8 = -3 \Rightarrow$ rewrite this operation $5 + (-8) = ? \pmod{13}$

$-8 \bmod 13 = 0 \bmod 13 - 8 \bmod 13 = (13 - 8) \bmod 13 = 5$

$8 - 8 = 8 + (-8) = (8 + 5) \bmod 13 = 13 \bmod 13 = 0$

Number 5 is additionally inverse to number 8 mod 13.

4) Division operation is defined in $Z_{13}^* = \{1, 2, 3, \dots, 12\}$
Let $z \in Z_{13}^*$, there exists unique number $z^{-1} = 1/z = 1:z$ such that
$z * z^{-1} = 1 \in Z_{13}^*$.
$u, v \in Z_{13} \Rightarrow u:v = u/v = u \cdot v^{-1} \mod 13$

Th. If p is prime, then multiplication and division operations are defined in $Z_p^* = \{1, 2, 3, \dots, p-1\}$
The element v^{-1} is called a multiplicatively inverse element to the element v in the set Z_p^*.
To divide u by v, the v^{-1} must be found.

>> mulinv (v, p) ⇒ ans >> v_m1 = mulinv(v, p)
>> mod (v * ans) = 1 mod p

Statement. Let n is an arbitrary number in N, then the addition and substraction operations mod n are defined in the set $Z_n = \{0, 1, 2, 3, \dots, n-1\}$

```
>> n = 27
>> a = 9
>> b = 15
>> mod (a + b, n)
>> mod (a - b, n)
>> mod (-b, n) ⇒ ans
>> mod (b + ans, n) = 0.
```

Exponent Table Z_{13}^*

	1	2	3	4	5	6	7	8	9	10	11	12
	2	4	8	3	6	12	11	9	5	10	7	1

$2^4 \mod 13 = 16 \mod 13 = 3$
$16 = 1 \cdot 13 + 3$

$2^e = 1, 2, 3, \dots, 12,$

1	2	3	4	5	6	7	8	9	10	11	12
2	4	8	3	6	12	11	9	5	10	7	1
3	9	1	3	9	1	3	9	1	3	9	1
4	3	12	9	10	1	4	3	12	9	10	1
5	12	8	1	5	12	8	1	5	12	8	1
6	10	8	9	2	12	7	3	5	4	11	1
7	10	5	9	11	12	6	3	8	4	2	1
8	12	5	1	8	12	5	1	8	12	5	1
9	3	1	9	3	1	9	3	1	9	3	1
10	9	12	3	4	1	10	9	12	3	4	1
11	4	5	3	7	12	2	9	8	10	6	1
12	1	12	1	12	1	12	1	12	1	12	1

$2^e = 1, 2, 3, \ldots, 12$,
when $e \in \{0, 1, 2, \ldots, 11\}$
$2^0 = 1$ & $2^{12} = 1$
2 – is a generator
of $Z_{13}^* = \{0, 1, 2, \ldots, 12\}$
$p = 13 = 2 \cdot 6 + 1$
$p = 11 = 2 \cdot 5 + 1$
q

A little corrected Table you can find below.

The set of generators $\Gamma = \{2, 6, 7, 11\}$ in Z_{13}^*.
In this case $p = 13$ and is prime.
$13 \longrightarrow 1101_b = 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 = 8 + 4 + 1 = 13.$
In cryptography the huge numbers p are used
$|13| = 4$ bits; $|p| = 2048$ bits $\Rightarrow p \sim 2^{2048} \approx 10^{600}$
In our Lab. W. We will use the numbers of 28 bit length to simulate crypto protocols.
$|p| = 28$ bits $|p| < 2^{28}$
>> 2^28 ; >> 2^30; >> 2^32 ;

$1K = 2^{10} = 1024$
$1M = 2^{20} = \ldots$
$1G = 2^{30} = \ldots$
$1T = 2^{40} = \ldots$

Multiplication Tab Z13*

*	1	2	3	4	5	6	7	8	9	10	11	12
1	1	2	3	4	5	6	7	8	9	10	11	12
2	2	4	6	8	10	12	1	3	5	7	9	11
3	3	6	9	12	2	5	8	11	1	4	7	10
4	4	8	12	3	7	11	2	6	10	1	5	9
5	5	10	2	7	12	4	9	1	6	11	3	8

6	6	12	5	11	4	10	3	9	2	8	1	7
7	7	1	8	2	9	3	10	4	11	5	12	6
8	8	3	11	6	1	9	4	12	7	2	10	5
9	9	5	1	10	6	2	11	7	3	12	8	4
10	10	7	4	1	11	8	5	2	12	9	6	3
11	11	9	7	5	3	1	12	10	8	6	4	2
12	12	11	10	9	8	7	6	5	4	3	2	1

Exponent Tab	Z13*												
^	0	1	2	3	4	5	6	7	8	9	10	11	12
1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	1	2	4	8	3	6	12	11	9	5	10	7	1
3	1	3	9	1	3	9	1	3	9	1	3	9	1
4	1	4	3	12	9	10	1	4	3	12	9	10	1
5	1	5	12	8	1	5	12	8	1	5	12	8	1
6	1	6	10	8	9	2	12	7	3	5	4	11	1
7	1	7	10	5	9	11	12	6	3	8	4	2	1
8	1	8	12	5	1	8	12	5	1	8	12	5	1
9	1	9	3	1	9	3	1	9	3	1	9	3	1
10	1	10	9	12	3	4	1	10	9	12	3	4	1
11	1	11	4	5	3	7	12	2	9	8	10	6	1
12	1	12	1	12	1	12	1	12	1	12	1	12	1