Kaunas University of Technology

Faculty of Mathematics and Natural Sciences

Cryptology

2nd laboratory work report

Marius Arlauskas

Digitally signed by Marius Arlauskas
Date: 2022.12.09 16:41:32 +02'00'

Marius Arlauskas 2022-12-09

Student

Assoc. prof. dr. Kęstutis Lukšys
Lecturer

Kaunas, 2022

1. Task 1

Task.

1. Write down a set of residue classes $\mathbb{Z}p$.

Results and comments.

Liekanų klasių aibė $\mathbb{Z}_{31}$: {0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30}

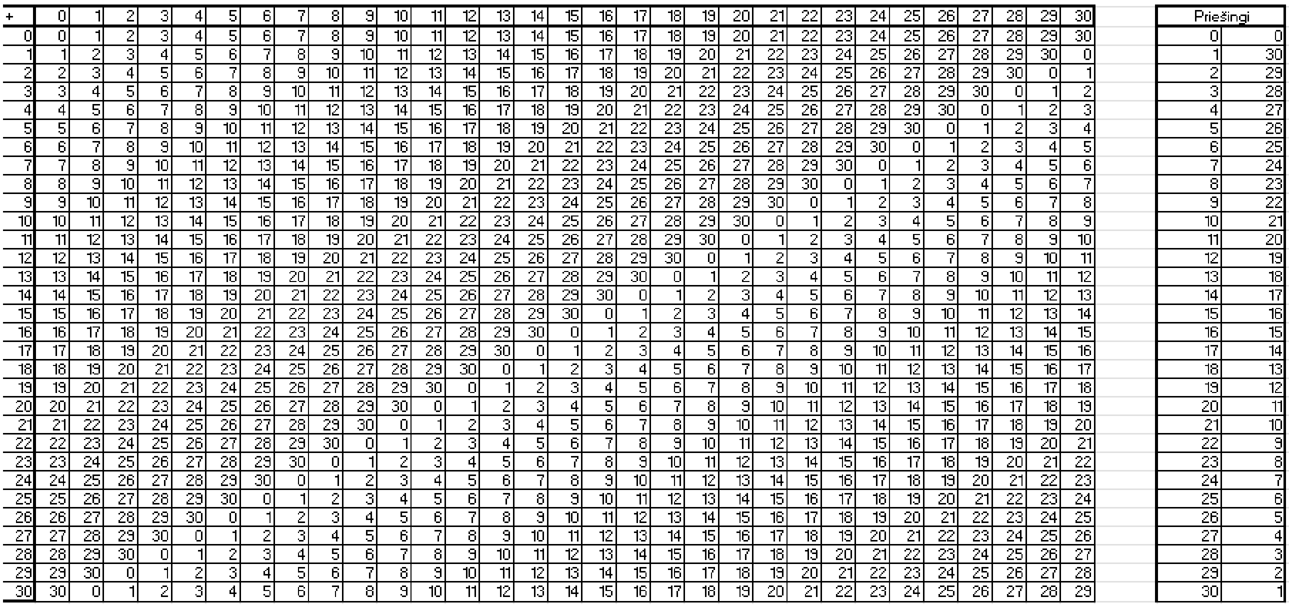
2. Task 2

Task.

Prepare addition and multiplication tables of residue ring $\langle \mathbb{Z}p; +,\cdot \rangle$. Find opposites and inverses for all elements.

Results and comments.

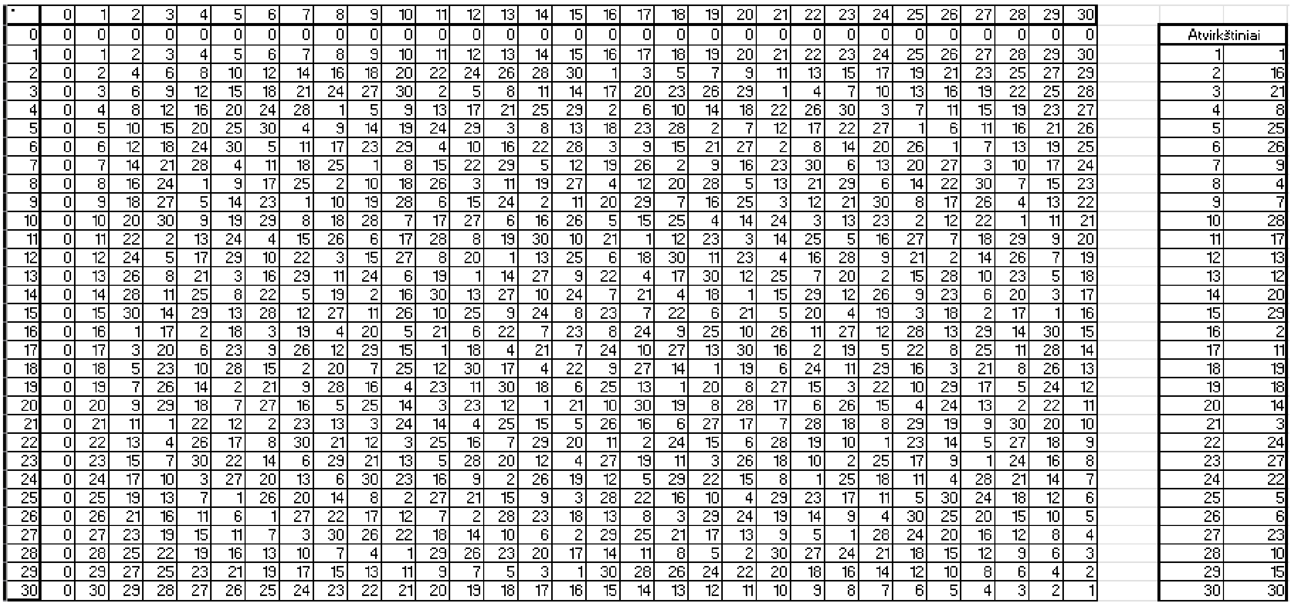
$\langle \mathbb{Z}_{31};\ + \rangle$, ir priešingi elementai:



+	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
0	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	0
2	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	0	1
3	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	0	1	2
4	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	0	1	2	3
5	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	0	1	2	3	4
6	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	0	1	2	3	4	5
7	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	0	1	2	3	4	5	6
8	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	0	1	2	3	4	5	6	7
9	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	0	1	2	3	4	5	6	7	8
10	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	0	1	2	3	4	5	6	7	8	9
11	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	0	1	2	3	4	5	6	7	8	9	10
12	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	0	1	2	3	4	5	6	7	8	9	10	11
13	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	0	1	2	3	4	5	6	7	8	9	10	11	12
14	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	0	1	2	3	4	5	6	7	8	9	10	11	12	13
15	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
16	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
17	17	18	19	20	21	22	23	24	25	26	27	28	29	30	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
18	18	19	20	21	22	23	24	25	26	27	28	29	30	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
19	19	20	21	22	23	24	25	26	27	28	29	30	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
20	20	21	22	23	24	25	26	27	28	29	30	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
21	21	22	23	24	25	26	27	28	29	30	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
22	22	23	24	25	26	27	28	29	30	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
23	23	24	25	26	27	28	29	30	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
24	24	25	26	27	28	29	30	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
25	25	26	27	28	29	30	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
26	26	27	28	29	30	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
27	27	28	29	30	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
28	28	29	30	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27
29	29	30	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
30	30	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29

Priešingi	
0	0
1	30
2	29
3	28
4	27
5	26
6	25
7	24
8	23
9	22
10	21
11	20
12	19
13	18
14	17
15	16
16	15
17	14
18	13
19	12
20	11
21	10
22	9
23	8
24	7
25	6
26	5
27	4
28	3
29	2
30	1

$\langle \mathbb{Z}_{31}; \cdot \rangle$, ir priešingi elementai:



*	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
2	0	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	1	3	5	7	9	11	13	15	17	19	21	23	25	27	29
3	0	3	6	9	12	15	18	21	24	27	30	2	5	8	11	14	17	20	23	26	29	1	4	7	10	13	16	19	22	25	28
4	0	4	8	12	16	20	24	28	1	5	9	13	17	21	25	29	2	6	10	14	18	22	26	30	3	7	11	15	19	23	27
5	0	5	10	15	20	25	30	4	9	14	19	24	29	3	8	13	18	23	28	2	7	12	17	22	27	1	6	11	16	21	26
6	0	6	12	18	24	30	5	11	17	23	29	4	10	16	22	28	3	9	15	21	27	2	8	14	20	26	1	7	13	19	25
7	0	7	14	21	28	4	11	18	25	1	8	15	22	29	5	12	19	26	2	9	16	23	30	6	13	20	27	3	10	17	24
8	0	8	16	24	1	9	17	25	2	10	18	26	3	11	19	27	4	12	20	28	5	13	21	29	6	14	22	30	7	15	23
9	0	9	18	27	5	14	23	1	10	19	28	6	15	24	2	11	20	29	7	16	25	3	12	21	30	8	17	26	4	13	22
10	0	10	20	30	9	19	29	8	18	28	7	17	27	6	16	26	5	15	25	4	14	24	3	13	23	2	12	22	1	11	21
11	0	11	22	2	13	24	4	15	26	6	17	28	8	19	30	10	21	1	12	23	3	14	25	5	16	27	7	18	29	9	20
12	0	12	24	5	17	29	10	22	3	15	27	8	20	1	13	25	6	18	30	11	23	4	16	28	9	21	2	14	26	7	19
13	0	13	26	8	21	3	16	29	11	24	6	19	1	14	27	9	22	4	17	30	12	25	7	20	2	15	28	10	23	5	18
14	0	14	28	11	25	8	22	5	19	2	16	30	13	27	10	24	7	21	4	18	1	15	29	12	26	9	23	6	20	3	17
15	0	15	30	14	29	13	28	12	27	11	26	10	25	9	24	8	23	7	22	6	21	5	20	4	19	3	18	2	17	1	16
16	0	16	1	17	2	18	3	19	4	20	5	21	6	22	7	23	8	24	9	25	10	26	11	27	12	28	13	29	14	30	15
17	0	17	3	20	6	23	9	26	12	29	15	1	18	4	21	7	24	10	27	13	30	16	2	19	5	22	8	25	11	28	14
18	0	18	5	23	10	28	15	2	20	7	25	12	30	17	4	22	9	27	14	1	19	6	24	11	29	16	3	21	8	26	13
19	0	19	7	26	14	2	21	9	28	16	4	23	11	30	18	6	25	13	1	20	8	27	15	3	22	10	29	17	5	24	12
20	0	20	9	29	18	7	27	16	5	25	14	3	23	12	1	21	10	30	19	8	28	17	6	26	15	4	24	13	2	22	11
21	0	21	11	1	22	12	2	23	13	3	24	14	4	25	15	5	26	16	6	27	17	7	28	18	8	29	19	9	30	20	10
22	0	22	13	4	26	17	8	30	21	12	3	25	16	7	29	20	11	2	24	15	6	28	19	10	1	23	14	5	27	18	9
23	0	23	15	7	30	22	14	6	29	21	13	5	28	20	12	4	27	19	11	3	26	18	10	2	25	17	9	1	24	16	8
24	0	24	17	10	3	27	20	13	6	30	23	16	9	2	26	19	12	5	29	22	15	8	1	25	18	11	4	28	21	14	7
25	0	25	19	13	7	1	26	20	14	8	2	27	21	15	9	3	28	22	16	10	4	29	23	17	11	5	30	24	18	12	6
26	0	26	21	16	11	6	1	27	22	17	12	7	2	28	23	18	13	8	3	29	24	19	14	9	4	30	25	20	15	10	5
27	0	27	23	19	15	11	7	3	30	26	22	18	14	10	6	2	29	25	21	17	13	9	5	1	28	24	20	16	12	8	4
28	0	28	25	22	19	16	13	10	7	4	1	29	26	23	20	17	14	11	8	5	2	30	27	24	21	18	15	12	9	6	3
29	0	29	27	25	23	21	19	17	15	13	11	9	7	5	3	1	30	28	26	24	22	20	18	16	14	12	10	8	6	4	2
30	0	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

Atvirkštiniai	
1	1
2	16
3	21
4	8
5	25
6	26
7	9
8	4
9	7
10	28
11	17
12	13
13	12
14	20
15	29
16	2
17	11
18	19
19	18
20	14
21	3
22	24
23	27
24	22
25	5
26	6
27	23
28	10
29	15
30	30

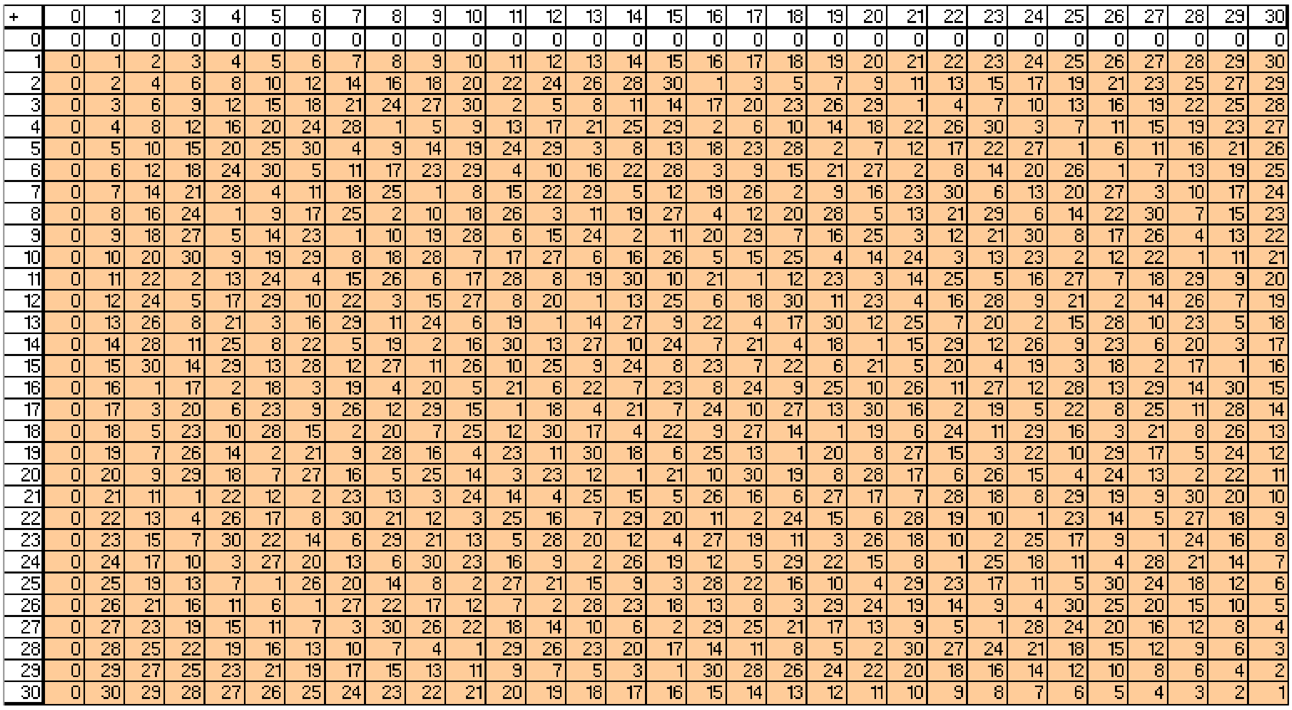
3. Task 2

Task.

How many generators are in group $\langle \mathbb{Z}p; +\rangle$? Find them.

Results and comments.

Sudėties operacijos laipsnių lentelė:



+	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
2	0	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	1	3	5	7	9	11	13	15	17	19	21	23	25	27	29
3	0	3	6	9	12	15	18	21	24	27	30	2	5	8	11	14	17	20	23	26	29	1	4	7	10	13	16	19	22	25	28
4	0	4	8	12	16	20	24	28	1	5	9	13	17	21	25	29	2	6	10	14	18	22	26	30	3	7	11	15	19	23	27
5	0	5	10	15	20	25	30	4	9	14	19	24	29	3	8	13	18	23	28	2	7	12	17	22	27	1	6	11	16	21	26
6	0	6	12	18	24	30	5	11	17	23	29	4	10	16	22	28	3	9	15	21	27	2	8	14	20	26	1	7	13	19	25
7	0	7	14	21	28	4	11	18	25	1	8	15	22	29	5	12	19	26	2	9	16	23	30	6	13	20	27	3	10	17	24
8	0	8	16	24	1	9	17	25	2	10	18	26	3	11	19	27	4	12	20	28	5	13	21	29	6	14	22	30	7	15	23
9	0	9	18	27	5	14	23	1	10	19	28	6	15	24	2	11	20	29	7	16	25	3	12	21	30	8	17	26	4	13	22
10	0	10	20	30	9	19	29	8	18	28	7	17	27	6	16	26	5	15	25	4	14	24	3	13	23	2	12	22	1	11	21
11	0	11	22	2	13	24	4	15	26	6	17	28	8	19	30	10	21	1	12	23	3	14	25	5	16	27	7	18	29	9	20
12	0	12	24	5	17	29	10	22	3	15	27	8	20	1	13	25	6	18	30	11	23	4	16	28	9	21	2	14	26	7	19
13	0	13	26	8	21	3	16	29	11	24	6	19	1	14	27	9	22	4	17	30	12	25	7	20	2	15	28	10	23	5	18
14	0	14	28	11	25	8	22	5	19	2	16	30	13	27	10	24	7	21	4	18	1	15	29	12	26	9	23	6	20	3	17
15	0	15	30	14	29	13	28	12	27	11	26	10	25	9	24	8	23	7	22	6	21	5	20	4	19	3	18	2	17	1	16
16	0	16	1	17	2	18	3	19	4	20	5	21	6	22	7	23	8	24	9	25	10	26	11	27	12	28	13	29	14	30	15
17	0	17	3	20	6	23	9	26	12	29	15	1	18	4	21	7	24	10	27	13	30	16	2	19	5	22	8	25	11	28	14
18	0	18	5	23	10	28	15	2	20	7	25	12	30	17	4	22	9	27	14	1	19	6	24	11	29	16	3	21	8	26	13
19	0	19	7	26	14	2	21	9	28	16	4	23	11	30	18	6	25	13	1	20	8	27	15	3	22	10	29	17	5	24	12
20	0	20	9	29	18	7	27	16	5	25	14	3	23	12	1	21	10	30	19	8	28	17	6	26	15	4	24	13	2	22	11
21	0	21	11	1	22	12	2	23	13	3	24	14	4	25	15	5	26	16	6	27	17	7	28	18	8	29	19	9	30	20	10
22	0	22	13	4	26	17	8	30	21	12	3	25	16	7	29	20	11	2	24	15	6	28	19	10	1	23	14	5	27	18	9
23	0	23	15	7	30	22	14	6	29	21	13	5	28	20	12	4	27	19	11	3	26	18	10	2	25	17	9	1	24	16	8
24	0	24	17	10	3	27	20	13	6	30	23	16	9	2	26	19	12	5	29	22	15	8	1	25	18	11	4	28	21	14	7
25	0	25	19	13	7	1	26	20	14	8	2	27	21	15	9	3	28	22	16	10	4	29	23	17	11	5	30	24	18	12	6
26	0	26	21	16	11	6	1	27	22	17	12	7	2	28	23	18	13	8	3	29	24	19	14	9	4	30	25	20	15	10	5
27	0	27	23	19	15	11	7	3	30	26	22	18	14	10	6	2	29	25	21	17	13	9	5	1	28	24	20	16	12	8	4
28	0	28	25	22	19	16	13	10	7	4	1	29	26	23	20	17	14	11	8	5	2	30	27	24	21	18	15	12	9	6	3
29	0	29	27	25	23	21	19	17	15	13	11	9	7	5	3	1	30	28	26	24	22	20	18	16	14	12	10	8	6	4	2
30	0	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

Generatoriai nustatomi iš laipsnių lentelės, kurioje reikšmės apskaičiuojamos moduliu 31 pvz: $2^4\,mod(31) = 2 + 2 + 2 + 2\,mod(31) = 2 \cdot 4\,mod(31)$. Visi sudietės aibės elementai yra generatoriai, nes sugeneruoja visus aibės elementus. Išskyrus 0, nes $0^n\ = 0 \cdot n\,mod(31)\ =\ 0$

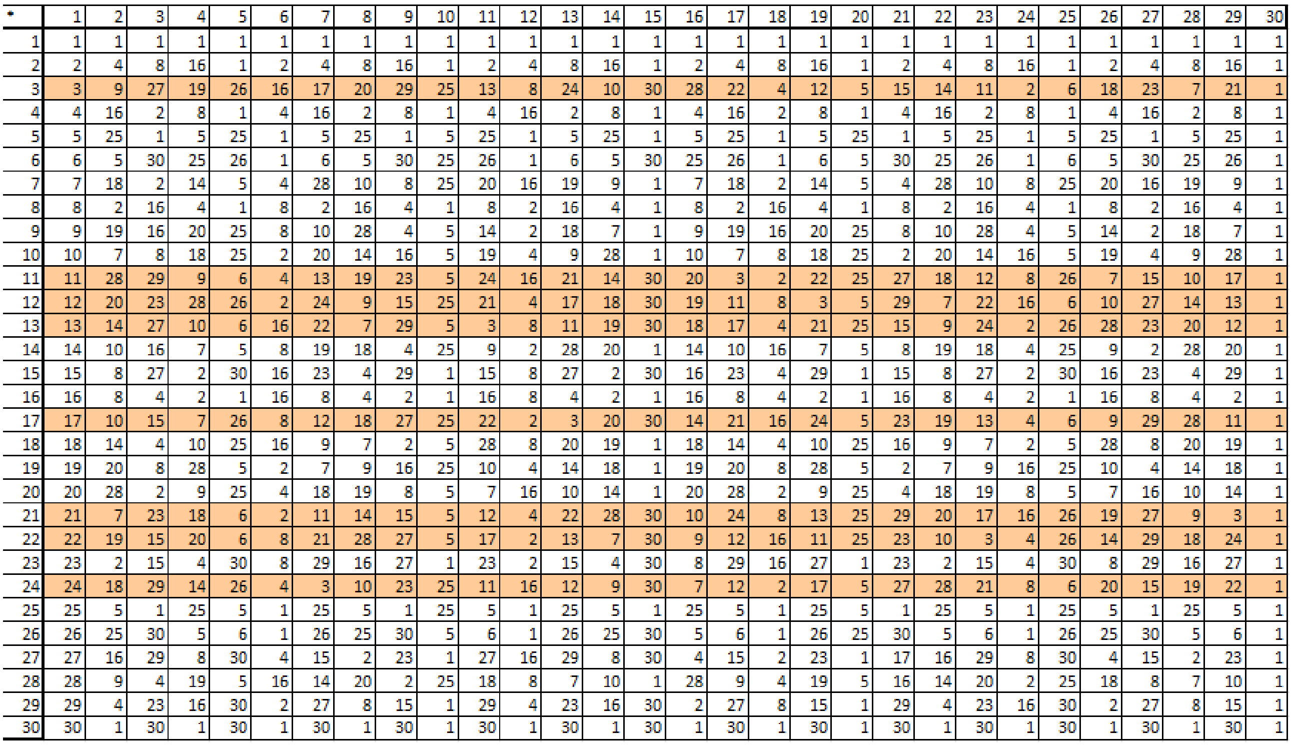
4. Task 2

Task.

How many generators are in group $\langle \mathbb{Z}p * ;\cdot\rangle$? Find them

Results and comments.

Daugybos operacijos laipsnių lentelė:



•	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	2	4	8	16	1	2	4	8	16	1	2	4	8	16	1	2	4	8	16	1	2	4	8	16	1	2	4	8	16	1
3	3	9	27	19	26	16	17	20	29	25	13	8	24	10	30	28	22	4	12	5	15	14	11	2	6	18	23	7	21	1
4	4	16	2	8	1	4	16	2	8	1	4	16	2	8	1	4	16	2	8	1	4	16	2	8	1	4	16	2	8	1
5	5	25	1	5	25	1	5	25	1	5	25	1	5	25	1	5	25	1	5	25	1	5	25	1	5	25	1	5	25	1
6	6	5	30	25	26	1	6	5	30	25	26	1	6	5	30	25	26	1	6	5	30	25	26	1	6	5	30	25	26	1
7	7	18	2	14	5	4	28	10	8	25	20	16	19	9	1	7	18	2	14	5	4	28	10	8	25	20	16	19	9	1
8	8	2	16	4	1	8	2	16	4	1	8	2	16	4	1	8	2	16	4	1	8	2	16	4	1	8	2	16	4	1
9	9	19	16	20	25	8	10	28	4	5	14	2	18	7	1	9	19	16	20	25	8	10	28	4	5	14	2	18	7	1
10	10	7	8	18	25	2	20	14	16	5	19	4	9	28	1	10	7	8	18	25	2	20	14	16	5	19	4	9	28	1
11	11	28	29	9	6	4	13	19	23	5	24	16	21	14	30	20	3	2	22	25	27	18	12	8	26	7	15	10	17	1
12	12	20	23	28	26	2	24	9	15	25	21	4	17	18	30	19	11	8	3	5	29	7	22	16	6	10	27	14	13	1
13	13	14	27	10	6	16	22	7	29	5	3	8	11	19	30	18	17	4	21	25	15	9	24	2	26	28	23	20	12	1
14	14	10	16	7	5	8	19	18	4	25	9	2	28	20	1	14	10	16	7	5	8	19	18	4	25	9	2	28	20	1
15	15	8	27	2	30	16	23	4	29	1	15	8	27	2	30	16	23	4	29	1	15	8	27	2	30	16	23	4	29	1
16	16	8	4	2	1	16	8	4	2	1	16	8	4	2	1	16	8	4	2	1	16	8	4	2	1	16	8	4	2	1
17	17	10	15	7	26	8	12	18	27	25	22	2	3	20	30	14	21	16	24	5	23	19	13	4	6	9	29	28	11	1
18	18	14	4	10	25	16	9	7	2	5	28	8	20	19	1	18	14	4	10	25	16	9	7	2	5	28	8	20	19	1
19	19	20	8	28	5	2	7	9	16	25	10	4	14	18	1	19	20	8	28	5	2	7	9	16	25	10	4	14	18	1
20	20	28	2	9	25	4	18	19	8	5	7	16	10	14	1	20	28	2	9	25	4	18	19	8	5	7	16	10	14	1
21	21	7	23	18	6	2	11	14	15	5	12	4	22	28	30	10	24	8	13	25	29	20	17	16	26	19	27	9	3	1
22	22	19	15	20	6	8	21	28	27	5	17	2	13	7	30	9	12	16	11	25	23	10	3	4	26	14	29	18	24	1
23	23	2	15	4	30	8	29	16	27	1	23	2	15	4	30	8	29	16	27	1	23	2	15	4	30	8	29	16	27	1
24	24	18	29	14	26	4	3	10	23	25	11	16	12	9	30	7	12	2	17	5	27	28	21	8	6	20	15	19	22	1
25	25	5	1	25	5	1	25	5	1	25	5	1	25	5	1	25	5	1	25	5	1	25	5	1	25	5	1	25	5	1
26	26	25	30	5	6	1	26	25	30	5	6	1	26	25	30	5	6	1	26	25	30	5	6	1	26	25	30	5	6	1
27	27	16	29	8	30	4	15	2	23	1	27	16	29	8	30	4	15	2	23	1	17	16	29	8	30	4	15	2	23	1
28	28	9	4	19	5	16	14	20	2	25	18	8	7	10	1	28	9	4	19	5	16	14	20	2	25	18	8	7	10	1
29	29	4	23	16	30	2	27	8	15	1	29	4	23	16	30	2	27	8	15	1	29	4	23	16	30	2	27	8	15	1
30	30	1	30	1	30	1	30	1	30	1	30	1	30	1	30	1	30	1	30	1	30	1	30	1	30	1	30	1	30	1

Generatorius, tai elementas, kuris sugeneruoja visus kitus grupės elementus, tai matome, kad šio atveju generatoriai yra 3, 11, 12, 13, 17, 21, 22, 24.

5. Task 2

Task.

Find subgroups of group $\langle \mathbb{Z}p * ;\cdot\rangle$ where all elements except 1 are generators and prove it (subgroup, generators).

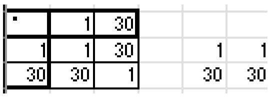
Results and comments.

Kad pogrupis būtų grupės $\langle \mathbb{Z}_{31} * ;\cdot\rangle$ pogrupiu, jis turi tenkinti šias sąlygas:

- Yra tenkinamas uždarumas (Dviejų pogrupio elementų sandauga priklauso pogrupiui).
- Pogrupio kiekvieno elemento atvirkštinis elementas priklauso pogrupiui. Taipogi pagal sąlygą visi elementai turi būti pogrupio generatoriais.

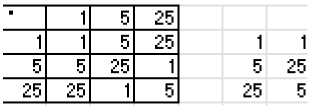
Rasti pogrupiai:

1) *{1, 30} – tenkina abi sąlygas.*



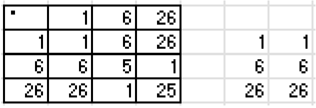
·	1	30			
1	1	30		1	1
30	30	1		30	30

2) {1, 5, 25} – *tenkina abi sąlygas.*



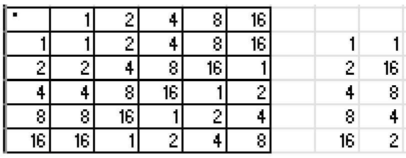
·	1	5	25			
1	1	5	25		1	1
5	5	25	1		5	25
25	25	1	5		25	5

3) {1, 6, 26} – *tenkina abi sąlygas.*



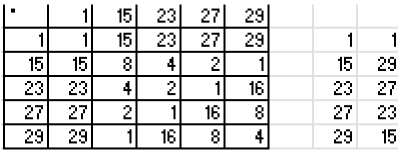
·	1	6	26			
1	1	6	26		1	1
6	6	5	1		6	6
26	26	1	25		26	26

4) {1, 2, 4, 8, 16} – *tenkina abi sąlygas.*



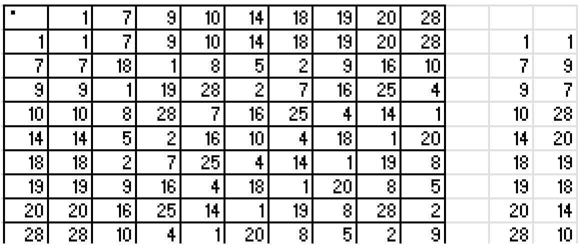
·	1	2	4	8	16			
1	1	2	4	8	16		1	1
2	2	4	8	16	1		2	16
4	4	8	16	1	2		4	8
8	8	16	1	2	4		8	4
16	16	1	2	4	8		16	2

5) {1, 15, 23, 27, 29} – *netenkina sąlygų.*



·	1	15	23	27	29			
1	1	15	23	27	29		1	1
15	15	8	4	2	1		15	29
23	23	4	2	1	16		23	27
27	27	2	1	16	8		27	23
29	29	1	16	8	4		29	15

6) {1, 7, 9, 10, 14, 18, 19, 20, 28} – *netenkina sąlygų.*



·	1	7	9	10	14	18	19	20	28			
1	1	7	9	10	14	18	19	20	28		1	1
7	7	18	1	8	5	2	9	16	10		7	9
9	9	1	19	28	2	7	16	25	4		9	7
10	10	8	28	7	16	25	4	14	1		10	28
14	14	5	2	16	10	4	18	1	20		14	20
18	18	2	7	25	4	14	1	19	8		18	19
19	19	9	16	4	18	1	20	8	5		19	18
20	20	16	25	14	1	19	8	28	2		20	14
28	28	10	4	1	20	8	5	2	9		28	10