Cryptology

Ryan Kellar

January 2024

1 Problem 1

1.1 a)

$\mathbb{Z}_n + \mathbb{Z}_m$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

1.2 b)

$\mathbb{Z}_n - \mathbb{Z}_m$	0	1	2	3	4	5
0	0	5	4	3	2	1
1	1	0	5	4	3	2
2	2	1	0	5	4	3
3	3	2	1	0	5	4
4	4	3	2	1	0	5
5	5	4	3	2	1	0

1.3 c)

$\mathbb{Z}_n * \mathbb{Z}_m$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

2 Problem 2

0, 1, 5, and 6

3 Problem 3

Because raising the number n to a power m signifies that we multiply n by itself m times (which is extremely repeated addition of n to itself). This means that, for this example, we can subtract 12 from 37 until we get an integer in the set $\mathbb{Z}_{12}$, which gives us 1 as the answer.

4 Problem 4

4

5 Problem 5

9

6 Problem 6

6.1 a)

25

6.2 b)

2

6.3 c)

25

7 Problem 7

7.1 a)

1

7.2 b)

1

7.3 c)

1

7.4 d)

1

7.5 e)

When you have an equation $a^k \bmod p$, if p and a are coprime, and $k = p - 1$, then no matter the values of a, k, and p, the answer will be 1.