Ochrona Danych – Laboratorium 2

Piotr Łasek, 235690

Zad 1 – przykładowa tabliczka mnożenia dla GF(8)

```
Tabliczka mnozenia:


0 0 0 0 0 0 0 0

0 1 a1 a2 a3 a4 a5 a6

0 a1 a2 a3 a4 a5 a6 1

0 a2 a3 a4 a5 a6 1 a1

0 a3 a4 a5 a6 1 a1 a2

0 a4 a5 a6 1 a1 a2 a3

0 a5 a6 1 a1 a2 a3 a4

0 a6 1 a1 a2 a3 a4 a5
```

Zad 2 – przykładowy wynik równania dla wprowadzonych danych

```
Wprowadz pierwsza liczbe: 2
Wprowadz druga liczbe: 2
Wprowadz p: 2
Wprowadz m: 2
Wynik dodawnia: 0
Wynik mnożenia: 3
```

Zad 3 – tabliczki mnożenia i dodawania dla GF(4), GF(8) i GF(16)

Tabliczka mnozenia	Tabliczka dodawania
0 0 0 0	0 1 2 3
0 1 2 3	1 0 3 2
0 2 3 1	2 3 0 1
0 3 1 2	3 2 1 0

Tabliczka mnozenia	Tabliczka dodawania
0 0 0 0 0 0 0 0	0 1 2 3 4 5 6 7
0 1 2 3 4 5 6 7	1 0 4 7 2 6 5 3
0 2 3 4 5 6 7 1	2 4 0 5 1 3 7 6
0 3 4 5 6 7 1 2	3 7 5 0 6 2 4 1
0 4 5 6 7 1 2 3	4 2 1 6 0 7 3 5
0 5 6 7 1 2 3 4	5 6 3 2 7 0 1 4
0 6 7 1 2 3 4 5	6 5 7 4 3 1 0 2
0 7 1 2 3 4 5 6	7 3 6 1 5 4 2 0

Tabliczka mnozenia	Tabliczka dodawania
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15	1 0 5 9 15 2 11 14 10 3 8 6 13 12 7 4
0 2 3 4 5 6 7 8 9 10 11 12 13 14 15 1	2 5 0 6 10 1 3 12 15 11 4 9 7 14 13 8
0 3 4 5 6 7 8 9 10 11 12 13 14 15 1 2	3 9 6 0 7 11 2 4 13 1 12 5 10 8 15 14
0 4 5 6 7 8 9 10 11 12 13 14 15 1 2 3	4 15 10 7 0 8 12 3 5 14 2 13 6 11 9 1
0 5 6 7 8 9 10 11 12 13 14 15 1 2 3 4	5 2 1 11 8 0 9 13 4 6 15 3 14 7 12 10
0 6 7 8 9 10 11 12 13 14 15 1 2 3 4 5	6 11 3 2 12 9 0 10 14 5 7 1 4 15 8 13
0 7 8 9 10 11 12 13 14 15 1 2 3 4 5 6	7 14 12 4 3 13 10 0 11 15 6 8 2 5 1 9
0 8 9 10 11 12 13 14 15 1 2 3 4 5 6 7	8 10 15 13 5 4 14 11 0 12 1 7 9 3 6 2
0 9 10 11 12 13 14 15 1 2 3 4 5 6 7 8	9 3 11 1 14 6 5 15 12 0 13 2 8 10 4 7
0 10 11 12 13 14 15 1 2 3 4 5 6 7 8 9	10 8 4 12 2 15 7 6 1 13 0 14 3 9 11 5
0 11 12 13 14 15 1 2 3 4 5 6 7 8 9 10	11 6 9 5 13 3 1 8 7 2 14 0 15 4 10 12
0 12 13 14 15 1 2 3 4 5 6 7 8 9 10 11	12 13 7 10 6 14 4 2 9 8 3 15 0 1 5 11
0 13 14 15 1 2 3 4 5 6 7 8 9 10 11 12	13 12 14 8 11 7 15 5 3 10 9 4 1 0 2 6
0 14 15 1 2 3 4 5 6 7 8 9 10 11 12 13	14 7 13 15 9 12 8 1 6 4 11 10 5 2 0 3
0 15 1 2 3 4 5 6 7 8 9 10 11 12 13 14	15 4 8 14 1 10 13 9 2 7 5 12 11 6 3 0