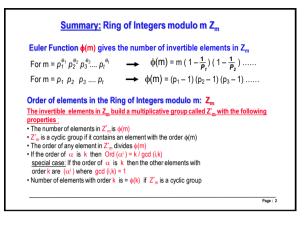
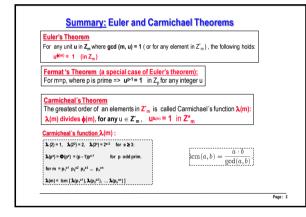
# Introduction to Cryptology

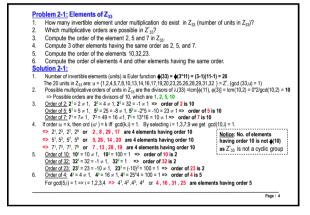
### Tutorial-2 Mathematical Background: Groups, Rings, Finite Fields (GF)

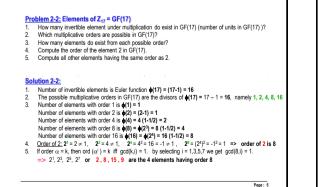
15.03.2023. v47

Page : 1









- Problem 2-3: Elements of GF(23) 1. How many invertible element under multiplic ion do exist GF(23) (number of units in GF(23) )? Which multiplicative orders are possible in GF(23)?

- Hindin manufacture of the possible in Or(20): How many elements do exist from each possible order? Compute the order of the element 2 in GF(23). Compute all other elements having the same order as 2. Compute his inverse of 2<sup>18</sup> in GF(23) <u>without</u> using the god algorithm. 6

### Solution 2-3:

3

- Number of invertible elements is Euler function (23) = (23-1) = 22 elements

- 5.
- 6.

Page : 6

- Homework:
   Elements of Z<sub>35</sub>

   1. How many invertible element under multiplication do exist Z<sub>35</sub> (number of units in Z<sub>35</sub>)?

   2. Which multiplicative orders are possible in Z'<sub>35</sub>?

   3. Compute the order of all invertible elements in Z'<sub>35</sub>.

   4. Find the cycle length for all non-invertible elements.

- Homework:
   Elements of Z<sub>39</sub>

   1. How many invertible element under multiplication do exist Z<sub>39</sub> (number of units in Z<sub>39</sub>)?

   2. Which multiplicative orders are possible in Z<sub>39</sub>?

   3. Compute the order of all invertible elements in Z<sub>39</sub>.

   4. Find the cycle length for all non-invertible elements.

## Homework: Analyze the structure of GF(29), GF(83), Z216

 $Z_{2^n}$  Is a widely used ring in modern cryptography

Page: 7