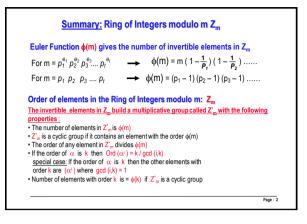
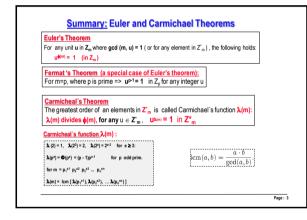
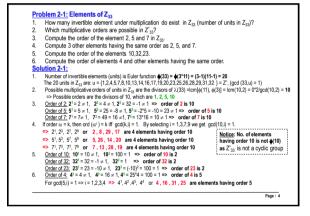
Introduction to Cryptology

Tutorial-02-1 Mathematical Background: Groups, Rings, Finite Fields (GF)

15.03.2023. v47







Problem 2-2: Elements of Z₁₇ = GF(17) How many invertible element under multiplication do exist in GF(17) (number of units in GF(17))? Which multiplicative orders are possible in GF(17)? How many elements do exist from each possible order? 2 Compute the order of the element 2 in GF(17). Compute all other elements having the same order as 2. 5 Solution 2-2: Number of invertible elements is Euler function (17) = (17-1) = 16 Number of invertible elements is Euler function $\phi(17) = (17 \cdot 1) = 16$ The possible multiplicative orders in GF(17) are the divisors of $\phi(17) = 17 - 1 = 16$, namely 1, 2, 4, 8, 16 Number of elements with order 1 is $\phi(1) = 1$ Number of elements with order 3 is $\phi(2) = (2 \cdot 1) = 1$ Number of elements with order 6 is $\phi(4) = 4(1 \cdot 12) = 2$ Number of elements with order 6 is $\phi(3) = \phi(2^2) = 8(1 \cdot 12) = 4$ Number of elements with order 6 is $\phi(3) = \phi(2^2) = 16(1 \cdot 12) = 8$ Order of 2 : $2^2 - 2^4$, $2^2 = 4 - 1$, $2^2 = 42^2 - 16 = 1 = 4^2$, $2^{2^2} = (2^4)^2 = -1^2 = 1 \Rightarrow$ order of 2 is 8 If order $\alpha = k$, then ord $(\alpha^i) = k$ iff god(ki) = 1. by selecting i = 1,3,5,7 we get god(8,i) = 1. $\Rightarrow 2^3$, 2^3 , 2^5 , 2^7 or 2, 8, 15, 9 are the 4 elements having order 8 5

Page : 5

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)?
- 3
- 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 2¹⁸ in GF(23) <u>without</u> using the god algorithm. 6

Solution 2-3:

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

- 5.
- 6.

Page : 6

- Homework:
 Elements of Z₃₅

 1. How many invertible element under multiplication do exist Z₃₅ (number of units in Z₃₅)?

 2. Which multiplicative orders are possible in Z'₃₅?

 3. Compute the order of all invertible elements in Z'₃₅.

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

- Homework:
 Elements of Z₃₉

 1. How many invertible element under multiplication do exist Z₃₉ (number of units in Z₃₉)?

 2. Which multiplicative orders are possible in Z₃₉?

 3. Compute the order of all invertible elements in Z₃₉.

 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