CSE3230 Algebra and Cryptography
Assignment A

2022-2023

1 Group of Invertible Elements (4%)

For each of the following $\langle \mathbb{Z}_m^*, \cdot \rangle$ give the elements in $\mathbb{Z}_m^*$ as well as the elements in U_m, and explain if they are groups or not. Please set the last number of your student number as x, e.g., 54019283, the last number is x=3. And then we have the following four groups:

- $\langle \mathbb{Z}_{1x}^*, \cdot \rangle$
- $\langle \mathbb{Z}_{2x}^*, \cdot \rangle$

For example, if x=3, then the groups are $\langle \mathbb{Z}_{13}^*, \cdot \rangle$ and $\langle \mathbb{Z}_{23}^*, \cdot \rangle$.

2 Order of an element of a group (6%)

For the following groups give the order of the elements in the group. Please set the second number x (from left to right) of your student number, e.g., 54019283, $x = 4$, and then we have the followings:

- $\langle \mathbb{Z}_{1x}, + \rangle$
- $\langle \mathbb{Z}_{2x}^*, \cdot \rangle$ (if $\langle \mathbb{Z}_{2x}^*, \cdot \rangle$ is not a group, round x to the closest digit such that it is a group)

For example, if $x = 3$, we will have $\langle \mathbb{Z}_{13}, + \rangle$ and $\langle \mathbb{Z}_{23}, \cdot \rangle$.

3 Euler's Totient Function ϕ (8%)

For each of the following $n \in \mathbb{N}$, compute $\phi(n)$, show intermediate steps in your computation. Please set the last two numbers of your student number as xy, e.g., 54019283, $xy = 83$. And then we have the followings:

- xy
- $2xy$
- $3xy7$
- $4xy1$

For example, if $xy = 83$, then we have the numbers $83, 283, 3837$ and 4831 to calculate their ϕ.

4 Subgroups (10%)

For the following statements state whether they are true or not, and explain/show why.

- $H = \{[1], [2], [4]\} \leq U_9$
- $H = \{[1], [2], [5]\} \leq U_9$

- $H = \{[1], [2], [4], [8]\} \leq U_9$
- $H = \{[1], [4], [7], [8]\} \leq U_9$
- $H = \{[1], [4], [5], [7], [8]\} \leq U_9$

5 Generator (12%)

Please choose the last number x of your student number, e.g., 54019287, $x = 7$.
1. List the generators of: (a) $\langle \mathbb{Z}_{1x}^*, \cdot \rangle$ (if $\langle \mathbb{Z}_{1x}^*, \cdot \rangle$ is not a group, round x to the closest digit such that it is a group); (b) $\langle \mathbb{Z}_{23}^*, \cdot \rangle$
2. List the elements of the subgroup $\langle x \rangle$ of $\langle \mathbb{Z}_{4x}^*, \cdot \rangle$. (if $\langle \mathbb{Z}_{4x}^*, \cdot \rangle$ is not a group, round x to the closest digit such that it is a group)
3. List the generators of the subgroup $\langle 3 \rangle$ of $\langle \mathbb{Z}_{31}^*, \cdot \rangle$.

6 Coset (6%)

Given U_{28} and $H = \{1, 9, 25\}$, list the cosets of H.

7 Homomorphism (20%)

For each of the following combination of groups and mapping φ state whether φ is a homomorphism and explain why. Where applicable also explain which type of homomorphism.

- Given $\langle \mathbb{Z}_6, + \rangle$ and $\langle U_{14}, \cdot \rangle$, let $\varphi : \mathbb{Z}_6 \to U_{14}$ be defined as $\varphi(a) = 3^a$
- Given $\langle \mathbb{Z}, + \rangle$ and $\langle G, \cdot \rangle$, where $G = \{1, -1\}$, let $\varphi : \mathbb{Z} \to G$ be defined as $\varphi(a) = \begin{cases} 1 & a \text{ is even} \\ -1 & a \text{ is odd} \end{cases}$
- Given $\langle \mathbb{R}^*, \cdot \rangle$, let $\varphi : \mathbb{R}^* \to \mathbb{R}^*$ be defined as $\varphi(a) = a^2$
- Given $\langle \mathbb{Z}_7^*, \cdot \rangle$, let $\varphi : \mathbb{Z}_7^* \to \mathbb{Z}_7^*$ be defined as $\varphi(a) = a$
- Given $\langle \mathbb{Z}, + \rangle$, let $\varphi : \mathbb{Z} \to \mathbb{Z}$ be defined as $\varphi(a) = 2a$

8 Representation of fields (20%)

- What are the additive, multiplicative, and vector representation for field elements $\mathbb{F}_{2^n}$ where $n = 3$ and primitive polynomial $x^3 + x + 1$?
- What are the additive, multiplicative, and vector representation for field elements $\mathbb{F}_{2^n}$ where $n = 3$ and primitive polynomial $x^3 + x^2 + 1$?
- What are the additive, multiplicative, and vector representation for field elements $\mathbb{F}_{2^n}$ where $n = 4$ and primitive polynomial $x^4 + x + 1$?
- Consider what happens when we use an irreducible polynomial instead of a primitive polynomial. As an example, you can use the irreducible polynomial $x^4 + x^3 + x^2 + x + 1$.

9 Irreducible or Reducible Polynomial (14%)

Let $f \in F_p[x]$ be an irreducible polynomial over F_p of degree m and with $f(0) \neq 0$. Then $\mathrm{ord}(f)$ is equal to the order of any root of f in the multiplicative group $F_{p^m}^*$.

(1) (7%) Please show that the polynomial $f(x) = x^6 + x^3 + 1$ is irreducible over F_2 and determine its order.

(2) (7%) Please show that the polynomial $f(x) = x^2 + 3x + 6$ is irreducible over F_7 and determine its order.