CSE3230 Algebra and Cryptography
Exercises - Block 3

March 31, 2023

1 Group of Invertible Elements (10%)

For each of the following group $\langle \mathbb{Z}_m^*, \cdot \rangle$ give the elements in this group as well as the elements in U_m. 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 $\langle \mathbb{Z}_{23}^*, \cdot \rangle$.

Solution:

- $\mathbb{Z}_X^*$ means all elements from 1 to X-1;
- $\mathbb{U}_X$ means all elements from 1 to X-1 which are relatively/co-prime with X.
- $\mathbb{Z}_{13}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$
  $U_{13} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$
- $\mathbb{Z}_{14}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13\}$
  $U_{14} = \{1, 3, 5, 9, 11, 13\}$
- $\mathbb{Z}_{16}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15\}$
  $U_{16} = \{1, 3, 5, 7, 9, 11, 13, 15\}$
- $\mathbb{Z}_{17}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16\}$
  $U_{17} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16\}$

2 Euler's Totient Function ϕ (10%)

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.

Solution:

http://www.javascripter.net/math/calculators/eulertotientfunction.htm Euler's totient function calculator;

3 Order of an element of a group (10%)

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:

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

For example, if $x = 4$, we will have $\langle \mathbb{Z}_{14}, + \rangle$ and $\langle \mathbb{Z}_{24}, \cdot \rangle$.

Solution:

- $\mathbb{Z}_X$ means that from 0 to X-1;
- $\mathbb{Z}_X^*$ means that from 1 to X-1;
- $\mathbb{Z}_{11} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$
- $\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$

4 Subgroups (10%)

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

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

Solution:

- False, $[2]^{-1} = [5] \notin H$
- False, $[2] \cdot [2] = [4] \notin H$
- False, $[2]^{-1} = [5] \notin H$
- False, $[4] \cdot [8] = [5] \notin H$
- False, $[5]^{-1} = [2] \notin H$

5 Generator (15%)

Please choose the last number x of your student number, e.g., 54019287, $x = 7$. Below is with operation "$\cdot$" .
1. List the generators of: (a) $\mathbb{Z}_{1x}$; for example, if $x = 7$, we have $\mathbb{Z}_{17}$; $(b)\mathrm{Z}_p$, where p is a prime.
2. List the elements of the subgroup $\langle x \rangle$ of $\mathbb{Z}_{4x}$.
3. List the generators of the subgroup $\langle 3 \rangle$ of $\mathbb{Z}_{27}$.

Solution:

1. (a) Generators are the elements from 1 to 1x-1 which are relatively prime to 1x.
2. Given the elements from 0 to 4x-1, the answers should be those elements can be divided by x.

6 Coset (5%)

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

Solution:

- $1H = \{1, 9, 25\} = H$
- $3H = \{3, 27, (2 \cdot 28) + 19\} = \{3, 27, 19\}$
- $5H = \{5, (28 \cdot 1) + 17, (28 \cdot 4) + 13\} = \{5, 17, 13\}$
- $9H = \{9, (28 \cdot 2) + 25, (28 \cdot 8) + 1\} = \{9, 25, 1\}$
- $11H = \{11, (28 \cdot 3) + 15, (28 \cdot 9) + 23\} = \{11, 15, 23\}$

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 $G = \{1, -1\}$, 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 $\varphi(a) = 2a$

Solution:

- φ is a homomorphism, for all $a, b \in \mathbb{Z}_6$, $\varphi(a + b) = 3^{a+b} = 3^a \cdot 3^b = \varphi(a) \cdot \varphi(b)$
  It is also an epimorphism, as it is surjective, all elements in the codomain have an element in the domain that maps to it:
  - $3^0 = [1]$ - $3^1 = [3]$ - $3^2 = [9]$ - $3^3 = [13]$ - $3^4 = [11]$ - $3^5 = [5]$

  Note that it is also isomorphic, 3 is a generator of U_{14}. It is not an endomorphism though, with that also not automorphism.
- φ is a homomorphism, we can show this using a proof by division into cases. Take arbitrary $a, b \in \mathbb{Z}$:
  - a is even and b is even, $a = 2m$ and $b = 2n$, where $m, n \in \mathbb{Z}$.
    $\varphi(2m + 2n) = \varphi(2(m + n)) = 1$
    $\varphi(2m) \cdot \varphi(2n) = 1 \cdot 1 = 1$
  - a is even and b is odd (or the other way around), $a = 2m$ and $b = 2n + 1$, where $m, n \in \mathbb{Z}$.
    $\varphi(2m + 2n + 1) = \varphi(2(m + n) + 1) = -1$
    $\varphi(2m) \cdot \varphi(2n + 1) = 1 \cdot -1 = -1$
  - a is odd and b is odd, $a = 2m + 1$ and $b = 2n + 1$, where $m, n \in \mathbb{Z}$.
    $\varphi(2m + 1 + 2n + 1) = \varphi(2(m + n + 1)) = 1$
    $\varphi(2m + 1) \cdot \varphi(2n + 1) = -1 \cdot -1 = 1$

  It is also an epimorphism, as each element in the codomain has an element in the domain that maps to it. It is not an isomorphism the order of the domain is larger than the order of the codomain. It is not an endomorphism or automorphism.
- φ is a homomorphism, for all $p, q \in \mathbb{R}^*$, $\varphi(p \cdot q) = (p \cdot q)^2 = p^2 \cdot q^2 = \varphi(p) \cdot \varphi(q)$
  It is not an epimorphism, negative numbers in $\mathbb{R}^*$ are not mapped to. It is an endomorphism though.
- φ is a homomorphism, for all $a, b \in \mathbb{Z}_7^*$, $\varphi(a \cdot b) = a \cdot b = \varphi(a) \cdot \varphi(b)$
  It is also an isomorphism and endomorphism, thus also an automorphism.
- φ is a homomorphism, for all $a, b \in \mathbb{Z}$, $\varphi(a + b) = 2(a + b) = 2a + 2b = \varphi(a) + \varphi(b)$
  It is not an epimorphism, only even integers are mapped to. It is an endomorphishm though.

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 $x^4 + x^3 + x^2 + x + 1$.

Solution:

Given $\mathbb{F}_{2^n}$ where $n = 3$ and primitive polynomial $x^3 + x + 1$:

mult.	0	1	α	α^2	α^3	α^4	α^5	α^6
add.	0	1	α	α^2	$\alpha+1$	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	α^2+1
vect.	000	001	010	100	011	110	111	101

Given $\mathbb{F}_{2^n}$ where $n = 3$ and primitive polynomial $x^3 + x^2 + 1$:

mult.	0	1	α	α^2	α^3	α^4	α^5	α^6
add.	0	1	α	α^2	α^2+1	$\alpha^2+\alpha+1$	$\alpha+1$	$\alpha^2+\alpha$
vect.	000	001	010	100	101	111	011	110

Given $\mathbb{F}_{2^n}$ where $n = 4$ and primitive polynomial $x^4 + x + 1$:

mult.	add.	vect.
0	0	0000
1	1	0001
α	α	0010
α^2	α^2	0100
α^3	α^3	1000
α^4	$\alpha+1$	0011
α^5	$\alpha^2+\alpha$	0110
α^6	$\alpha^3+\alpha^2$	1100
α^7	$\alpha^3+\alpha+1$	1011
α^8	α^2+1	0101
α^9	$\alpha^3+\alpha$	1010
α^{10}	$\alpha^2+\alpha+1$	0111
α^{11}	$\alpha^3+\alpha^2+\alpha$	1110
α^{12}	$\alpha^3+\alpha^2+\alpha+1$	1111
α^{13}	$\alpha^3+\alpha^2+1$	1101
α^{14}	α^3+1	1001

Given $\mathbb{F}_{2^n}$ where $n = 4$ and primitive polynomial $x^4 + x^3 + x^2 + x + 1$:

mult.	add.	vect.
0	0	0000
1	1	0001
α	α	0010
α^2	α^2	0100
α^3	α^3	1000
α^4	$\alpha^3+\alpha^2+\alpha+1$	1111
α^5	1	0001
α^6	α	0010
α^7	α^2	0100
α^8	α^3	1000
α^9	$\alpha^3+\alpha^2+\alpha+1$	1111
α^{10}	1	0001
α^{11}	α	0010
α^{12}	α^2	0100
α^{13}	α^3	1000
α^{14}	$\alpha^3+\alpha^2+\alpha+1$	1111

9 Irreducible or Reducible Polynomial (14%)

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

(1) (7%) Please show that the polynomial $f(x) = x^6 + x^3 + 1$ is irreducible over $_2$ and determine its order.

(2) (7%) Please show that the polynomial $f(x) = x^2 + 3x + 6$ is irreducible over $_7$ and determine its order.

Marking: 3 points for using root approach; 2-4 points for using degree 1,2,3...testing, depending on the given answers.

Solution:

Let $f(x) = x^6 + x^3 + 1 \in_2 [x]$.

Polynomial f is irreducible if and only if there is no $h(x) \in_2 [x]$ with degree $1 \leq \deg(h) \leq 3$ such that $h(x) \mid f(x)$. Hence, we need to check if f can be divided by a polynomial $h(x)$ of degree $1 \leq \deg(h) \leq 3$. We do not need to consider the polynomials without a constant term (i.e. without a "+1") since f has it, and thus its supposed factors must also have it. Therefore, the polynomial factors to be used in the divisions are:

- Degree 1: $x + 1$
- Degree 2: $x^2 + 1$, $x^2 + x + 1$
- Degree 3: $x^3 + 1$, $x^3 + x + 1$, $x^3 + x^2 + 1$, $x^3 + x^2 + x + 1$

We need to check 7 divisions, namely:

- $f = x^6 + x^3 + 1 = (x^5 + x^4 + x^3)(x + 1) + red1$
- $f = x^6 + x^3 + 1 = (x^4 + x^2 + x + 1)(x^2 + 1) + redx$
- $f = x^6 + x^3 + 1 = (x^4 + x^3)(x^2 + x + 1) + red1$
- $f = x^6 + x^3 + 1 = x^3 \cdot (x^3 + 1) + red1$
- $f = x^6 + x^3 + 1 = (x^3 + x)(x^3 + x + 1) + redx^2 + x + 1$
- $f = x^6 + x^3 + 1 = (x^3 + x^2 + x + 1)(x^3 + x^2 + 1) + redx$
- $f = x^6 + x^3 + 1 = (x^3 + x^2 + 1)(x^3 + x^2 + x + 1) + redx$

Since none of the above remainders is 0, polynomial $x^6 + x^3 + 1$ is irreducible over $_2$. Note using root approach could be given 3%.

To determine the order of f, we need to compute the order of one of its roots α in the multiplicative group $^*_{2^6}$. We have that

$$\alpha^7 = \alpha \cdot \alpha^6 = \alpha \cdot (\alpha^3 + 1) = \alpha^4 + \alpha,$$
$$\alpha^8 = \alpha \cdot \alpha^7 = \alpha \cdot (\alpha^4 + \alpha) = \alpha^5 + \alpha^2,$$
$$\alpha^9 = \alpha \cdot \alpha^8 = \alpha \cdot (\alpha^5 + \alpha^2) = \alpha^6 + \alpha^3 = 1.$$

Therefore, ord$(f) = 9$. (2%)

Let $f(x) = x^2 + 3x + 6 \in_7 [x]$.

As polynomial f has degree 2, it is irreducible if and only if f has no roots in $_7$. Therefore,

- $f(0) = 0^2 + 3 \cdot 0 + 6 = red6$
- $f(1) = 1^2 + 3 \cdot 1 + 6 = red3$
- $f(2) = 2^2 + 3 \cdot 2 + 6 = red2$
- $f(3) = 3^2 + 3 \cdot 3 + 6 = red3$
- $f(4) = 4^2 + 3 \cdot 4 + 6 = red6$
- $f(5) = 5^2 + 3 \cdot 5 + 6 = red4$
- $f(6) = 6^2 + 3 \cdot 6 + 6 = red4$

Since none of the above evaluations is 0, polynomial $x^2 + 3x + 6$ is irreducible over $_7$. Note using root approach can be given 3%.

To determine the order of f, we need to compute the order of one of its roots α in the multiplicative group $^*_{7^2}$. We have that

$$\alpha^3 = 3\alpha + 4, \quad \alpha^4 = 2\alpha + 3, \quad \alpha^5 = 4\alpha + 2, \quad \alpha^6 = 4\alpha + 4, \quad \alpha^7 = 6\alpha + 4, \quad \alpha^8 = 6, \quad \alpha^9 = 6\alpha,$$
$$\alpha^{10} = 3\alpha + 6, \quad \alpha^{11} = 4\alpha + 3, \quad \alpha^{12} = 5\alpha + 4, \quad \alpha^{13} = 3\alpha + 5, \quad \alpha^{14} = 3\alpha + 3, \quad \alpha^{15} = \alpha + 3, \quad \alpha^{16} = 1.$$

Therefore, ord$(f) = 16$. (2%)