University of Bergen
Faculty of Mathematics and Natural Sciences

INF 240 - Basic Tools for Coding theory and Cryptography - Midterm Preparation
Solutions to the exercises

Problem 1. *1. A **group** is a pair $(S, *)$ of a set S and a binary operation $* : S \times S \to S$ (in other words, an operation which takes two elements of S as inputs and outputs one element as S) which satisfies the following axioms:*

*(i) the operation is **associative**, i.e. $a * (b * c) = (a * b) * c$ for any $a, b, c \in S$;*

*(ii) there is an element $e \in S$ which satisfies $a * e = e * a = a$ for any $a \in S$; this element is called the **identity element** or **neutral element**;*

*(iii) for each element $a \in S$ there is an element a^{-1} which satisfies $a * a^{-1} = \bar{a} * a = e$; this is called the **inverse** of a.*

2. The Cayley tables for addition, resp. multiplication over $\mathbb{Z}_7$ are given under Table 1, resp. Table 2 below.

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

Table 1: Cayley table for $(\mathbb{Z}_7, +)$

*	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Table 2: Cayley table for $(\mathbb{Z}_7, \cdot)$

3. *To verify that $(\mathbb{Z}_7, +)$ is a group, we have to check that the three axioms from the definition (associativity, identity, inverse) hold. Since addition modulo 7 is simply ordinary addition over $\mathbb{Z}$ followed by modulation, and since we know that ordinary addition over $\mathbb{Z}$ is associative, then so is addition modulo 7. In other words, since $a + (b + c) = (a+b)+c$ over $\mathbb{Z}$, then also $(a+(b+c)) \mod 7 = ((a+b)+c) \mod 7$ since the inputs to the modulation operation are the same. Clearly, 0 is the neutral element with respect to addition, since $a+0 = 0+a = a$ for any a. Finally, to make sure that every element has an inverse, it is enough to verify that each row and each column of Table 1 contains the neutral element 0; this is indeed the case, and so $(\mathbb{Z}_7, +)$ is a group.*

4. *The identity element with respect to multiplication is 1. If we look at Table 2, we see that the column corresponding to 0 does not contain 1 anywhere; thus, no matter what we multiply 0 by, we will never get the identity. In conclusion, 0 does not have an inverse, and hence $(\mathbb{Z}_7, \cdot)$ is not a group.*

5. *Since 7 is a prime, and the size of any subgroup S of a group G is a divisor of the size of G, a subgroup of $(\mathbb{Z}_7, +)$ can only contain 1 or 7 elements, i.e. $(\mathbb{Z}_7, +)$ can only have the trivial subgroup $\{0\}$ consisting of the identity element, and the entire group $\mathbb{Z}_7$ itself as subgroups. For the purpose of providing more insight into the working of subgroups, we find a normal subgroup of $(\mathbb{Z}_8, +)$ instead; since 1, 2, 4, and 8 are all divisors of 8, the group $(\mathbb{Z}_8, +)$ can have non-trivial subgroups.*

   We know that every subgroup must contain the identity element (in this case, 0), and must be closed under addition. Suppose our group contains 0 and 1; since it is closed under addition, the elements $2 = 1+1$, $3 = 1+1+1$, etc. must also belong to the subgroup. We thus get that the subgroup must be $\mathbb{Z}_7$ itself. Suppose now that we take 0 and 2 to be elements of the subgroup. Then also $4 = 2+2$ and $6 = 2+2+2$ must be in the subgroup as well. Now, if we take the set $S = \{0, 2, 4, 6\}$, we can see that it is closed under addition since the sum of any two *elements is already in S, e.g.* $6+6=4 \in S$, $2+4=6 \in S$. *A subgroup must also be closed under the inverse operation, and, in this case, it is easy to verify that this is indeed so:* $-0=0$, $-2=6$, $-4=4$, *and* $-6=2$ *are all in* S.

In general, a subgroup S of G is called ***normal*** *if* $g*h*g^{-1} \in S$ *for any* $h \in S$ *and any* $g \in G$, *where* g^{-1} *denotes the inverse of* g. *In this case, however, we do not have to check this. We know that any subgroup of an Abelian, or commutative, group (one where* $a*b=b*a$ *for all possible* a *and* b*) is normal; since addition is a commutative operation, our* $S=\{0,2,4,6\}$ *is automatically a normal subgroup of* $\mathbb{Z}_8$.

6. *The factor group* $(\mathbb{Z}_8,+)/S$ *consists of classes, and two elements* $a,b \in \mathbb{Z}_8$ *belong to the same class if and only if* $a-b \in S$, *where* $-b$ *is the inverse of* b *under addition. We see that e.g.* 0 *and* 1 *belong to different classes since* $1-0 \notin S$, *while* 2 *and* 0 *are in the same class since* $2-0 \in S$. *In the end, we only get two classes:* $[0]=\{0,2,4,6\}$ *and* $[1]=\{1,3,5,7\}$. *Thus* $(\mathbb{Z}_8,+)/S=\{[0],[1]\}$. *To perform addition of two classes* $[x]$ *and* $[y]$ *in the factor group, we simply compute the sum* $x+y$ *of the elements which represent them and find the class which contains the sum. For example,* $[1]+[1]=[1+1]=[2]=[0]$ *since* 0 *and* 2 *belong to the same class.*

7. *The* ***order*** *of a group or subgroup is the number of its elements; here the order of* S *is* 4. *The* ***index*** *of a subgroup* S *of a group* G *is the number of elements in the factor group* G/S*; in this case, the index of* S *in* $\mathbb{Z}_8$ *is* 2. *Note that the product of the order and the index of any subgroup* S *of a group* G *is always equal to the order of* G: $4 \cdot 2 = 8$.

8. *We now go back to* $\mathbb{Z}_7$. *A* ***generator*** *is an element* g *such that applying the group operation to* g *enough times produces every element of the group. We already observed that* 1 *generates* $(\mathbb{Z}_7,+)$ *since taking* 1, $1+1=2$, $1+1+1=3$, $\ldots$, $1+1+1+1+1+1=6$ *gives us all elements. In the case of* $(\mathbb{Z}_7 \setminus \{0\},\cdot)$ *we can see that taking* 2, $2\cdot2=4$, $2\cdot2\cdot2=1$ *only produces three elements, so* 2 *is not a generator. But taking* 3, $2=3\cdot3$, $6=3^3$, $4=3^4$, $5=3^5$, $1=3^6$ *yields all non-zero elements in* $\mathbb{Z}_7$, *so* 3 *is a generator of* $(\mathbb{Z}_7 \setminus \{0\},\cdot)$.

Problem 2.

1. *A* ***monic polynomial*** *is one whose most significant coefficient (the one in front of the term of highest degree) is equal to* 1. *Here* $f(x)$ *is not monic but* $g(x)$ *is.*

2. *The degree of* $f(x)$ *is the value of the largest exponent with a non-zero coefficient. Here* $\deg(f)=5$ *and* $\deg(g)=3$.

3. *We have*

$$f(x) = g(x) = 2x^5 + x^3 + (1 + 2)x + (2 + 2) = 2x^5 + x^3 + 3x + 4.$$

Note that all computations involving coefficients are performed modulo 7 since the polynomial is in $\mathbb{F}_7[x]$. The exponents, however, are not modulated.

4. *We have*

$$(2x^5+x+2)(x^3+2x+2) = 2x^8+2x^6+4x^5+x^4+2x^2+2x+2x^3+4x+4 = 2x^8 + 2x^6 + 4x^5 + x^4 + 2x^3 + 2x^2 + 6x + 4.$$

Once again, all computations are performed modulo 7.

5. *We get $2x^5 + x + 2 = (x^3 + 2x + 2)(2x^2 + 3) + 3x^2 + 2x + 3$.*

Problem 3. 1. *An **irreducible polynomial** $f(x)$ is one that cannot be written as the product $f(x) = g(x)h(x)$ of two other polynomials satisfying both $\deg(g) < \deg(f)$ and $\deg(h) < \deg(f)$.*

2. *We write down all polynomials over $\mathbb{F}_2[x]$ of degree 3. These are all polynomials of the form $x^3 + ax^2 + bx + c$ for $a, b, c \in \mathbb{F}_2$:*

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

Since these polynomials are of degree 3, if they are reducible, then one of the factors $g(x)$ and $h(x)$ must be of degree 1, and we know that any polynomial divisible by a polynomial of degree 1 has a root. It thus suffices to filter out the polynomials from the list that have roots. We only have two possible values, viz. 0 and 1, which may be roots, so this is easy to check. In the end, we are left with only $x^3 + x + 1$ and $x^3 + x^2 + 1$.

3. *Let $p(x) = x^3 + x + 1$. The finite field $\mathbb{E} = \mathbb{F}_2[x]/(p(x))$ consists of classes represented by all possible remainders of division by $p(x) = x^3+x+1$, i.e. all polynomials of degree at most 2, i.e. all polynomials of the form $ax^2 + bx + c$ for $a, b, c \in \mathbb{F}_2$:*

$$\mathbb{E} = \{[0], [1], [x], [x + 1], [x^2], [x^2 + 1], [x^2 + x], [x^2 + x + 1]\}.$$

4. *To compute sums or products of* $[x]$ *and* $[y]$*, we simply compute* $x+y$*, resp.* $x \cdot y$ *and modulate by* $p(x)$ *if necessary. We thus have*

$$[x+1]+[x^2+x]=[x^2+1],$$

$$[x+1]+[x^2+x+1]=[x^2],$$

$$[x^2+x]+[x^2+x+1]=[1],$$

$$[x+1]\cdot[x^2+x]=[1],$$

$$[x+1]\cdot[x^2+x+1]=[x],$$

$$[x^2+x]\cdot[x^2+x+1]=[x^2].$$

5. *The additive inverse* $-[x]$ *of* $[x]$ *is simply the class* $[-x]$*; in this case, addition and subtraction are the same, i.e.* $-1 = 1 \mod 2$*, so every element is its own additive inverse.*

6. *To be a multiplicative inverse to* $a=[x+1]$*, the element* d *would have to satisfy* $[x+1]\cdot d = d \cdot [x+1] = [1]$*.*