University of Bergen
Faculty of Mathematics and Natural Sciences

INF 240 - Basic Tools for Coding theory and Cryptography - Midterm Preparation

February 25, 2020 Student number: _____

Allowed assistance: Textbooks, lecture notes, calculators.

Problem 1. *1. Give the definition of a group.*

2. *Construct Cayley tables for* $(\mathbb{Z}_7, +)$ *and* $(\mathbb{Z}_7, \cdot)$*, with addition and multiplication modulo 7.*

3. *Using the Cayley table for* $(\mathbb{Z}_7, +)$*, verify that it is a group.*

4. *Using the Cayley table for* $(\mathbb{Z}_7, \cdot)$*, verify that it is not a group.*

5. *Find a normal subgroup* N *of* $(\mathbb{Z}_7, +)$*.*

6. *Construct the factor group* $(\mathbb{Z}_7, +)/N$*. Explain how to perform addition in the factor group.*

7. *Find the index and the order of* N *in* $(\mathbb{Z}_7, +)$*.*

8. *Find generators of* $(\mathbb{Z}_7, +)$ *and* $(\mathbb{Z}_7, \cdot)$*.*

Problem 2. *Consider the polynomials* $f(x) = 2x^5 + x + 2$ *and* $g(x) = x^3 + 2x + 2$ *in* $\mathbb{F}_7[x]$.

1. *Give the definition of a monic polynomial. Are* $f(x)$ *and* $g(x)$ *monic?*
2. *Give the definition of the degree* $\deg(f)$ *of a polynomial* $f(x)$. *What are the degrees of* $f(x)$ *and* $g(x)$*?*
3. *Compute the sum* $f(x) + g(x)$.
4. *Compute the product* $f(x) \cdot g(x)$.
5. *Divide* $f(x)$ *by* $g(x)$ *with remainder, i.e. find polynomials* $q(x)$ *and* $r(x)$ *in* $\mathbb{F}_7[x]$ *such that* $f(x) = q(x) \cdot g(x) + r(x)$ *and* $\deg(r) < \deg(g)$.

Problem 3. *Consider the polynomial ring* $\mathbb{F}_2[x]$.

1. *Give the definition of an irreducible polynomial.*
2. *Find all irreducible polynomials in* $\mathbb{F}_2[x]$ *of degree* 3.
3. *Take* $p(x)$ *to be one of the irreducible polynomials from the previous step. Use it to construct the extension field* $\mathbb{E} = \mathbb{F}_2[x]/(p(x))$.
4. *Consider the elements* $a = [x+1]$, $b = [x^2+x]$, *and* $c = [x^2+x+1]$ *of* $\mathbb{E}$. *Compute the sums* $a+b$, $a+c$, $b+c$ *and the products* ab, ac, bc.
5. *What are the additive inverses of* a, b, *and* c*?*
6. *What would an element* $d \in \mathbb{E}$ *have to satisfy in order for it to be a multiplicative inverse to e.g.* a*?*