S-72.341 CODING METHODS

Tutorial 2

1. (Wicker, problem 2.22) List all possible orders taken on by the elements in the field GF(125) and determine the number of elements in the field that display each allowed order.

2. (Wicker, problems 2.36, 3.7) Let α be a primitive element of GF(1024).
   a) List the elements in the subfield GF(4) and GF(32) as powers of α.
   b) Find the conjugates of α with respect to the subfields GF(2), GF(4), GF(32).

3. (Wicker, problem 3.3). Express the following pairs $(f(x), g(x))$ of binary polynomials in the form $f(x) = m(x)g(x) + r(x)$.
   a) $\left(x^8 + 1, x^4 + 1\right)$
   b) $\left(x^8 + 1, x^4 + x\right)$
   c) $\left(x^{10} + x^9 + x^5 + x^4, x + 1\right)$
   d) $\left(x^5 + x^3 + 1,\ x^2 + x + 1\right)$.

4. (Wicker, problem 3.11). Determine the degree of the minimal polynomial with respect to GF(2) for field elements with the following orders:
   a) 9
   b) 13
   c) 21
   d) 1023.

5. (Exam 15.5.2001) The field GF(4) may be constructed by taking the primitive polynomial $f(x) = x^2 + x + 1 \in \mathrm{GF}(2)[x]$ and letting α be a root of $f(x)$. Then the elements of the field are $F = \left\{0, 1 = \alpha^0, \alpha^1, \alpha^2\right\}$. **Task:** Give complete addition and multiplication tables for GF(4). For the elements in these tables, it is required that you use the elements in the aforementioned set F.

6. Construct addition and multiplication tables for GF(8) using the primitive polynomial $f(x) = x^3 + x + 1$.

7. (Exam 9.1.2002) Algebra.

   a) Express $x^3 + 1 \in \mathrm{GF}(2)[x]$ as a product of binary irreducible polynomials.

   b) Multiply $x^2 + x + 1$ and $x^2 + x + 2$ in the ring $\mathrm{GF}(3)[x]/\left(x^3 - 1\right)$.

8. (Wicker, problem 3.12). Express the following polynomials over GF(2) as the products of irreducible polynomials:

   a) $x^7 + 1$

   b) $x^{15} + 1$

   c) $x^{21} + 1$