S-72.341 Coding Methods (3 cr) P spring 2004

Home Assignment 1: Finite Fields

There are two mandatory tasks (task 1 and task2), for which detailed solutions are required. The third task is optional, but gives extra points for the exam. Depending on your student number, **solve only one instance of each task**. Let your student number be *abcde*F ($0 \leq a, b, c, d, e \leq 9$, F a letter). For the first task, solve instance j, where $a+b+c+d+e \equiv j \pmod 4$. For the second task, solve instance i, where $i \equiv e \pmod 5$. For the third task, solve instance i, where $i \equiv d \pmod 5$

1. Determine whether the following polynomial is primitive in GF(2)[x]:
   (0) x^5+x^2+1; (1) x^4+x+1; (2) x^3+x^2+1; (3) x^2+x+1.

2. Determine whether the following polynomial from GF(3)[x] is irreducible:
   (0) $x^5+x^4+x^3+1$; (1) $x^5+x^3+x^2+x+1$; (2) $x^4+2x^3+2x^2+x+1$;
   (3) x^3+x^2+x+1; (4) x^4+x^2+1.

   Bonus task (optional)

3. Factoring x^n-1. Determinate the number of binary irreducible polynomials in the factorization of the following:
   (0) x^9+1; (1) $x^{11}+1$; (2) $x^{13}+1$; (3) $x^{17}+1$; (4) $x^{19}+1$.

Return your solutions into the box underneath the bulletin-board of the course no later than March 3, 2004. Remember to include all your personal data. Co-operation is not allowed.