Institut für Mathematische Optimierung
TU Braunschweig

SS 2006

Prof. Dr. Sándor Fekete
Nils Schweer

Coding Theory / Discrete Mathematics II
Assignment 5 (June 1, 2006)

(This assignment is due on June 15, 2006, 1.00 p.m., by dropping it into the wooden box **in front of** F 310)

Exercise 1 (Product $\bmod f(x)$**):**

Because $f(x) = 1+x+x^3$ is an irreducible polynomial from $\mathbb{Z}_2[x]$, we know from Theorem 3.7 that $\mathbb{Z}_2(f)$ is a field. $g(x) = 1 + x + x^2$ and $h(x) = 1 + x^2$ are two elements of $\mathbb{Z}_2(f)$. Compute the sum and the product $(\bmod f(x))$ of $g(x)$ and $h(x)$.

(2+13 Points)

Exercise 2 (Proof of Theorem 3.7**):**

Complete the proof of Theorem 3.7 by adding all necessary details.

(20 Points)

Exercise 3 (Irreducible polynomial):

Let $f(x) = a_m x^m + a_{m-1}x^{m-1} + \ldots + a_0$ with $a_i \in \mathbb{Z}$. Let p be a prime number with the following properties: p does not divide a_m, p divides $a_{m-1}, \ldots, a_0$ and p^2 does not divide a_0. Show that f is irreducible over $\mathbb{Z}$.
(Hint: Suppose f is reducible. How are the coefficients $a_0, \ldots, a_m$ determined? Try to find a contradiction to the first property of p.)

(25 Points)