Mathematics 392 – Seminar in Coding Theory
Individual Problem Set 3
April 3, 2002

The following problems will be due Wednesday, April 10.

From the text

- 5.1.15 b,c,d
- 5.1.16
- 5.1.17
- 5.1.18
- 5.2.8

Additional Problems

A) (A detail in proving our formula for idempotents) Let n be an odd number and let $0 \leq j \leq n-1$. Show that if $m \equiv \overline{m} \bmod n$, then $x^m \equiv x^{\overline{m}} \bmod x^n + 1$.

B) This problem will introduce some of the ideas behind a proof that there exist irreducible polynomials of every positive degree in $\mathbf{F}_2[x]$. The ideas will depend on the use of *generating functions*. Given a sequence a_n, $n \geq 0$, the generating function of this sequence is the power series

$$\sum_{n=0}^{\infty} a_n t_n = a_0 + a_1 t + a_2 t^2 + \cdots$$

1) (a "warmup") Consider the sequence $a_n =$ *number of different ways of making a total of n cents using only pennies, nickels, and dimes.* (Take $a_0 = 1$ by definition.) For instance, $a_7 = 2$, since we can make a total of 7 cents either with 7 pennies, or with one nickel and two pennies. Work out the values of a_n for all $n \leq 20$, and show that these values match the coefficents of the corresponding terms t^n in the expansion of

$$\left(\sum_{n=0}^{\infty} t^n\right)\left(\sum_{n=0}^{\infty} t^{5n}\right)\left(\sum_{n=0}^{\infty} t^{10n}\right) = (1 + t + t^2 + \cdots)(1 + t^5 + t^{10} + \cdots)(1 + t^{10} + t^{20} + \cdots)$$
$$= \frac{1}{1-t} \cdot \frac{1}{1-t^5} \cdot \frac{1}{1-t^{10}}$$

(where the last line comes from using the geometric series summation formula). Explain why this expansion equals the generating function of our sequence here.

2) Now consider the generating function for the sequence $a_n =$ number of polynomials of degree exactly n in $\mathbf{F}_2[x]$. What does this function look like. Try to

express it as a rational function using the geometric series summation formula as in part 1.

3) It is a standard theorem from the algebra of polynomials that every monic polynomial in $\mathbf{F}_2[x]$ can be factored *uniquely* into a product of irreducibles. Show that this implies that your generating function from part 2 is equal to a product similar to the one in part 1, but with infinitely many terms:

$$\prod_{r=1}^{\infty} \left(\frac{1}{1-t^r} \right)^{N_r}$$

where N_r is the *number of irreducible polynomials of degree exactly* r *in* $\mathbf{F}_2[x]$.

4) Set your answers for parts 2 and 3 equal to each other, take logarithms of both sides, and differentiate. By comparing coefficients of like powers of t in the resulting equation, deduce that

$$2^n = \sum_{r|n, 0<r<n} r N_r .$$

(From this, with a little cleverness, it can be shown that $N_r > 0$ for all $r \geq 1$, so irreducible polynomials of all degrees exist.)