

MATH 4450/6450
HOMEWORK 9
DUE 4/13/07

Do the following book problems:

18.12: 11, 12, 13, 18, 19, 20.

18.13: 1.

Your instructions for the extra problems this week are: 4450 students should do Extra Problems 1, 2, and 3. As usual, 6450 students have to do everything.

Extra Problem 1: If $f(x) = a_0 + a_1x + \dots + a_dx^d$ is a polynomial in $\mathbb{F}_q[x]$, define the *reciprocal polynomial* $f_r(x)$ to be the polynomial $a_0x^d + a_1x^{d-1} + \dots + a_d$.

(a) Suppose that $a_0 \neq 0$. Show that α is a root of f if and only if $1/\alpha$ is a root of f_r . (The multiplicities match up too...why?) That explains the name.

(b) Show that $f(x)$ is a divisor of $x^n - 1$ if and only if $f_r(x)$ is. (Don't use part (a). It might be a little tricky if there were multiple roots.)

(c) Suppose that $f(x)h(x) = x^n - 1$ and f is monic. Let C be the cyclic code generated by f . Show that C^\perp is cyclic also and $h_r(x)/h(0)$ is a generating polynomial for it. (Hint: this should follow immediately from something we said in class.)

Extra Problem 2: (a) (This is a fact you may have seen before, but we'll need it below.) Let $f(x)$ be a polynomial in $\mathbb{F}[x]$, where \mathbb{F} is any field. Show that if $\gcd(f(x), f'(x)) = 1$, then $f(x)$ cannot have a repeated factor (i.e. there is no polynomial $g(x)$ such that $g(x)^2$ divides $f(x)$). (Yes, that's the derivative there!)

(b) Let p be a prime, and let q be a power of p . Show that $x^n - 1$ has no repeated factors over \mathbb{F}_q if and only if $p \nmid n$. (Remember, it's an if and only if statement!)

Extra Problem 3: In this problem we consider binary cyclic codes C . We say that a polynomial $e(x) \in \mathbb{F}_2[x]$ of degree $\leq n - 1$ is an *n-idempotent* if $e(x)^2 \equiv e(x) \pmod{x^n - 1}$. Our goal will be to prove the following

Theorem: Let C be a binary cyclic code of odd length n . Then there is an *n-idempotent* polynomial $e(x)$ such that the codewords of C correspond to the multiples of $e(x) \pmod{x^n - 1}$.

(Note that this does not contradict the uniqueness in the theorem about cyclic codes that we proved in class, because we are not assuming that $e(x)$ is a divisor of $x^n - 1$; the theorem we proved in class says that a cyclic code has a unique monic generating polynomial that is a divisor of $x^n - 1$.) We call the $e(x)$ produced by the theorem an *n-idempotent generator*.

(a) First, as a warmup: how many 5-idempotents are there? Write them down. Then do the same thing for $n = 7$. (Hint: if $e(x) = e_0 + \dots + e_6x^6$, then we can write down $e(x)^2$ very simply. Remember that we're working mod 2! Aside: you might think about what happens in the general case. How can you tell how many n -idempotents there will be?)

(b) On to the proof of the theorem. First step: factor $x^n - 1 = g(x)h(x)$, where $g(x)$ is the generating polynomial for our binary cyclic code C . Since $g(x)$ and $h(x)$ are relatively prime (explain why this is true!), we can write $a(x)g(x) + b(x)h(x) = 1$ for some $a(x), b(x) \in \mathbb{F}_2[x]$. Show that $a(x)g(x) \bmod x^n - 1$ is an n -idempotent.

(c) Call the n -idempotent we discovered above $e(x)$; then $e(x)$ corresponds to a codeword in C . Show that if $c(x)$ is a polynomial corresponding to a codeword of C , then $c(x)e(x) \equiv c(x) \bmod x^n - 1$. Explain why this shows that $e(x)$ is an n -idempotent generator for C .

(d) As a bonus, show that if C is an $[n, k]$ code, then the $k \times n$ matrix formed by taking the vector corresponding to $e(x)$ as the first row and then letting the $(i + 1)$ st row be the cyclic shift of the i th row ($1 \leq i \leq k - 1$) is a generating matrix for C . (Hint: it's enough to show that it has rank k .)

Extra Problem 4: (a) Suppose $e(x)$ is an n -idempotent generator for a binary cyclic code C . Let $c(x)$ be a polynomial corresponding to a codeword of C . Show that $c(x)e(x) \equiv c(x) \bmod x^n - 1$. (This is essentially the converse of Extra Problem 3(c).)

To set up the rest of this problem, recall from linear algebra that if C_1 and C_2 are codes, then $C_1 \cap C_2$ and $C_1 + C_2$ are also codes. Now suppose that C_1 is a binary cyclic code of length n with generating polynomial $g_1(x)$ and n -idempotent generator $e_1(x)$, and that C_2 is a binary cyclic code of length n with generating polynomial $g_2(x)$ and n -idempotent generator $e_2(x)$.

(b) Show that $C_1 \cap C_2$ is a binary cyclic code of length n with generating polynomial $\text{lcm}[g_1(x), g_2(x)]$ and n -idempotent generator $e_1(x)e_2(x)$. (Hint for the second part: by the work you did in Extra Problem 3(c), it's enough to show that $c(x)e_1(x)e_2(x) \equiv c(x) \bmod x^n - 1$ for any polynomial $c(x)$ corresponding to a codeword in $C_1 \cap C_2$.)

(c) Show that $C_1 + C_2$ is a binary cyclic code of length n with generating polynomial $\text{gcd}(g_1(x), g_2(x))$ and n -idempotent generator $e_1(x) + e_2(x) - e_1(x)e_2(x)$.

Extra Problem 5: If you've seen this one before, don't complain—just write your answer down and count yourself lucky.

Let x_1, \dots, x_n be elements of a field \mathbb{F} . Let M be the $n \times n$ matrix whose ij entry is x_j^{i-1} , so

$$M = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ x_1 & x_2 & \cdots & x_n \\ x_1^2 & x_2^2 & \cdots & x_n^2 \\ \vdots & \vdots & \vdots & \vdots \\ x_1^{n-1} & x_2^{n-1} & \cdots & x_n^{n-1} \end{bmatrix}.$$

Show that

$$\det(M) = \prod_{1 \leq i < j \leq n} (x_j - x_i).$$

(Hint: let $p(x) = \prod_{k=1}^{n-1} (x - x_k)$. Show that you can do row operations to M , without changing the determinant, until the last row of M is

$$[p(x_1) \quad p(x_2) \quad \cdots \quad p(x_n)] = [0 \quad 0 \quad \cdots \quad 0 \quad p(x_n)].$$

Now use properties of the determinant and induct on n .)