Math 5251 Error-correcting codes and finite fields
Spring 2006, Vic Reiner
Midterm exam 2- Due Wednesday April 5, in class

Instructions: This is an open book, open library, open notes, open web, take-home exam, but you are *not* allowed to collaborate. The instructor is the only human source you are allowed to consult.

1. (20 points total)
(a) (10 points) We know $\alpha = \overline{10}$ in $\mathbb{F}_{47}$ has a multiplicative inverse α^{-1}. Find α^{-1} explicitly, using Euclid's algorithm.
(b) (10 points) We know that $f(x) = x^2$ and $g(x) = x^3 + x + 1$ in $\mathbb{F}_2[x]$ are relatively prime. Hence there will exist some polynomials $a(x), b(x) \in \mathbb{F}_2[x]$ satisfying $a(x)f(x) + b(x)g(x) = 1$. Find a, b explicitly, using Euclid's algorithm.

2. (20 points total) My friend and I set up a cyclic redundancy check system using the generator $g(x) = x^3 + x^2 + 1$ in $\mathbb{F}_2[x]$.

(a) (5 points) I want to send my friend the message with bits 111000, by tacking on three extra bits a, b, c and sending $111000abc$ in such a way that the CRC my friend computes from this will be 0. What are a, b, c?
(b) (5 points) For this $g(x)$, will single bit errors in a message always be detected? Explain why, or give an example where this fails.
(c) (5 points) For this $g(x)$, will odd numbers of bit errors in a message always be detected? Explain why, or give an example where this fails.
(d) (5 points) Consider two-bit errors in which the two positions containing the errors are exactly N bits aparts. What is the smallest value of N for which such a two-bit error will be undetected by $g(x)$?

3. (24 points total) Let G be the following matrix

$$G = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

(a) (8 points) Think of the three rows of G as vectors in $(\mathbb{F}_2)^6$, generating a binary code $\mathcal{C}_1$ equal to the row space of G over $\mathbb{F}_2$. What is the (binary) rate of $\mathcal{C}_1$?
(b) (8 points) What is the minimum distance of $\mathcal{C}_1$, and up to how many errors can it correct?

(c) (8 points) Think of the three rows of G as vectors in $(\mathbb{F}_3)^6$, generating a ternary code $\mathcal{C}_2$ equal to the row space of G, this time over $\mathbb{F}_3$, not $\mathbb{F}_2$. What is the (ternary) rate of $\mathcal{C}_2$?

4. (10 points) Let m be a composite number, say with a nontrivial factorization $m = pq$. Show that the ring $\mathbb{Z}/m[x]$ fails to have unique factorization, by exhibiting a quadratic (i.e. degree two) polynomial $f(x)$ in $\mathbb{Z}/m[x]$ having two *different* factorizations into linear factors (and exhibit those two factorizations).

5.(10 points total)
(a) (2 points) For each of these elements of $\mathbb{F}_p$, compute a representative in $\mathbb{F}_p$ in the range $\{0, 1, \ldots, p-1\}$:

$$\begin{array}{ccc} (3-1)! & = 2! & \text{in } \mathbb{F}_3, \\ (5-1)! & = 4! & \text{in } \mathbb{F}_5, \\ (7-1)! & = 6! & \text{in } \mathbb{F}_7, \\ (11-1)! & = 10! & \text{in } \mathbb{F}_{11}. \end{array}$$

(b) (3 points) Conjecture a simple formula (involving no sums nor products) for the residue $(p-1)!$ in $\mathbb{F}_p$ when p is a prime.
(c) (5 points) Prove your conjecture from part (b).
(A possible hint for (d): recall that we showed

$$(x-1)(x-2)\cdots(x-(p-1)) = x^{p-1} - 1$$

in $\mathbb{F}_p[x]$).

6. (16 points total) Recall that for a ring R, a subset I of R is called an *ideal* if I is closed under

- addition, meaning that $a, b \in I$ implies $a + b \in I$, and
- multiplication by elements of R, meaning that $a \in I, r \in R$ implies $ra \in I$.

(a) (10 points) Prove that if R is a field then it has exactly two ideals, namely $I_1 = \{0\}$ and $I_2 = R$ itself.
(b) (6 points) Prove the converse: if a ring R has exactly two ideals (namely $I_1 = \{0\}$ and $I_2 = R$ itself), then R is a field.