C&O 331: Assignment #2

Due date: Feb 1 (Wednesday)

1. Let $q \geq 2$, and let n and d be positive integers with $d \leq n$. Let $T_q(n,d)$ denote the maximum integer M for which there exists an $[n,M]$-block code of distance d over an alphabet of size q.

   (a) Prove that $T_q(n,d) \leq q^n$ for all $1 \leq d \leq n$.

   (b) Prove that $T_q(n,1) = q^n$.

   (c) Prove that $T_q(n,n) = q$.

2. The polynomial $f(x) = x^5 + 4x + 2$ is irreducible over $\mathbb{Z}_5$.

   (a) What is the order of the field $F = \mathbb{Z}_5[x]/(f(x))$?

   (b) Describe, in words, the elements of the field F.

   (c) What is the characteristic of the field F?

   (d) Perform the following computation in F: $(4x^4 + 3x^2 + x + 3) \; + \; (3x^4 + 4x^3 + 2x^2 + 1)$.

   (e) Use the extended Euclidean algorithm for polynomials to find the (multiplicative) inverse of the element $a = 2x^2 + 3$.

   (f) Perform the following computation in F: $(x+4)^5 \cdot (4x^3 + 2x^2 + x + 4)^{6249}$.

3. Recall the *division algorithm for polynomials:* Let F be a field and let $f,\, g \in F[x]$, with $g \neq 0$. Then long division of f by g yields unique polynomials $l, r \in F[x]$ such that

$$f = lg + r, \text{ where } \deg(r) < \deg(g).$$

   (a) Prove the *Factor Theorem*: The linear polynomial $x - a \in F[x]$ is a factor of $f \in F[x]$ if and only if $f(a) = 0$.

   (b) Find all irreducible polynomials of degrees 1, 2, 3 and 4 over $GF(2)$.

4. Let $f(x) = x^3 + 2x + 2$.

   (a) Prove that $f(x)$ is irreducible over $\mathbb{Z}_3$.

   (b) In the field $GF(3^3)$ defined by $f(x)$, the element x has order 13. Find a primitive element in this field. (Justify your answer.)

   (c) List all of the possible orders of elements in $GF(3^3)^*$ and the number of elements of these particular orders.

5. Let $\alpha \in GF(q)^*$. The *order* of α, denoted $\mathrm{ord}(\alpha)$, is the smallest positive integer t such that $\alpha^t = 1$. Note that $\mathrm{ord}(\alpha)$ exists since $\alpha^{q-1} = 1$. Now, suppose that $\mathrm{ord}(\alpha) = t$.

   (a) Prove that the elements $\alpha^0, \alpha^1, \ldots, \alpha^{t-1}$ are pairwise distinct.

   (b) Let s be an integer. Prove that $\alpha^s = 1$ if and only if $t \mid s$. (Hint: Use the division algorithm for integers to write $s = qt + r$, where $0 \leq r < t$.)

   (c) Prove that $\mathrm{ord}(\alpha) = \mathrm{ord}(\alpha^{-1})$.

Please note that assignments are not weighted equally. Each problem on each assignment is worth 10 marks. The total marks received on assignments will be added together at the end of the course.

You should make an effort to solve all the problems on your own. You are also welcome to collaborate with your colleagues, and to seek assistance from the teaching assistant or the instructor. However, *all solutions must be written up by yourself*. If you do collaborate, please acknowledge your collaborators in the write-up for each problem. *If you obtain a solution with help from a book, solutions from previous offerings of the course, a web site (including Wikipedia), or elsewhere, please acknowledge your source.*

The assignment is due by 5:00pm on February 1. Late assignments will not be accepted except in very special circumstances.