Math 342, Spring Term 2009
Final Exam

April 16^{th},2009

ID: ____

Name: ____

Signature: ____

Instructions

- Do not turn this page over until instructed.
- You will have 150 minutes for this exam.
- No books, notes or electronic devices.
- Solutions should be written clearly, in complete English sentences, showing all your work.
- If you use a result from the lectures or the problem sets, quote it properly.

1		/25
2		/25
3		/15
4		/15
5		/15
6		/5
Total		/100

1 The integers (25 points)

a. Find all integer solutions to the equation $12x \equiv 4\,(80)$ **(10 pts).**
Hint: $7 \cdot 3 = 21$**.**

b. Find a zero-divisor in $\mathbb{Z}/10\mathbb{Z}$ **(5 pts).**

c. Let p **be a prime number. What are the possible values for** $\gcd(a, p)$ **if** $a \in \mathbb{Z}$**? (5 pts)**

d. For p prime use Bezout's Theorem to show that $\mathbb{Z}/p\mathbb{Z}$ is a field (5 pts).

2 Linear codes (25 points)

a. Define the *weight* of a vector $\underline{v} \in F^n$**. Define the *weight* of a subspace** $C \subset F^n$ **(7 pts)**

b. Let $C_3 \subset \mathbb{F}_2^8$ **be the set of linear combinations of the three bit vectors** $\underline{a} = (11000011)$, $\underline{b} = (00110011)$, $\underline{c} = (00001111)$. **Show that the code** C_3 **has weight** 4 **(7 pts)**

c. Let $G \in M_{7\times 3}(\mathbb{F}_2)$ be the matrix below, and let $C_{\mathbf{H}} = \left\{ G \begin{pmatrix} x \\ y \\ z \end{pmatrix} \middle| x, y, z \in \mathbb{F}_2 \right\} \subset \mathbb{F}_2^7$ be the code for which G is the generating matrix. Show that $C_{\mathbf{H}}$ has weight 4 (7 pts).

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

d. Both codes C_3 and $C_{\mathbf{H}}$ can be used to encode a data-stream by breaking the data into 3-bit blocks. Which code is better? Why? (4 pts)

3 Polynomials (15 points)

a. CRC-Encode the following 9-bit vectors using the polynomial $F_4(x) = x^4 + x + 1 \in \mathbb{F}_2[x]$ **(8 pts).**

1. (000000000)

2. (100100001)

b. Find the gcd of the two real polynomials $x^3 + x^2 + 3x - 5$ **and** $x^2 - 1$ **(7 pts).**

4 Maps of algebraic structures (15 points)

For a 3×3 matrix $A \in M_3(\mathbb{R})$ set $\mathrm{Tr}(A) = A_{11} + A_{22} + A_{33}$ (sum of the diagonal), which defines a map $\mathrm{Tr}\colon M_3(\mathbb{R}) \to \mathbb{R}$. We can give the domain and range different algebraic structures. For each of these structures you need to decide whether this map is a homomorphism of that kind of structure (prove your answers!)

a. First, is Tr a group homomorphism from group $(M_3(\mathbb{R}), 0_3, +)$ to the group $(\mathbb{R}, 0, +)$? (5 pts)

b. Next, think of $M_3(\mathbb{R})$ as an 9-dimensional real vector space in the usual way. Is $\mathrm{Tr}\colon M_3(\mathbb{R}) \to \mathbb{R}^1$ a linear map? (5 pts)

c. Finally, give both $M_3(\mathbb{R})$ and $\mathbb{R}$ their usual ring structures. Is $\mathrm{Tr}\colon M_3(\mathbb{R}) \to \mathbb{R}$ a homomorphism of rings? (5 pts)

5 RSA (15 points)

Consider the RSA cryptosystem with modulus $m = 21$ and encoding exponent $e = 5$.

a. Find the order $\varphi(m)$ of the group $(\mathbb{Z}/m\mathbb{Z})^\times$ (4 pts).

b. Find the decoding exponent d (4 pts).

c. Decode the messages $[4]_{21}$, $[5]_{21}$ (7 pts).

6 Last problem (5 points)

Show that the real function $\sqrt{x^4 + x^2}$ is not of the form $\frac{f(x)}{g(x)}$ where f, g are non-zero polynomials with real coefficients.