Math 342, Fall Term 2011
Final Exam

December 9^{th},2011

Student number:

LAST name:

First name:

Signature:

Instructions

- Do not turn this page over. You will have 150 minutes for the exam.
- You may not use books, notes or electronic devices of any kind.
- Solutions should be written clearly, in complete English sentences, showing all your work.
- If you are using a result from the textbook, the lectures or the problem sets, state it properly.

1	/15
2	/10
3	/25
4	/10
5	/15
6	/15
7	/10
Total	/100

1 (15 points)

a. Define "a is invertible in the commutative ring R" and exhibit a unit in $\mathbb{Z}/30\mathbb{Z}$. (10 points)

b. Use Euclid's algorithm to calculate $\gcd(120, 14)$. (5 points)

2 (10 points)

In this problem we consider the map $f\colon \mathbb{Z}/30\mathbb{Z} \to \mathbb{Z}/5\mathbb{Z}$ given by

$$f\left([n]_{30}\right) = [n+2]_5 \,.$$

a. Assume that $[n]_{30} = [m]_{30}$. Show that $[n+2]_5 = [m+2]_5$. (5 points)

b. Is f a group homomorphism (for the addition operation)? Why or why not? (5 points)

3 A Linear Code (25 points)

In this problem we work over the field with 7 elements, denoted $\mathbb{F}_7$ or $\mathbb{Z}/7\mathbb{Z}$.
Let $H \in M_{3\times 7}(\mathbb{F}_7)$ be the following matrix:

$$H = \begin{pmatrix} 1 & 1 & 0 & 1 & -1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & -1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & -1 \end{pmatrix}$$

and let $C_H = \left\{ \underline{v} \in \mathbb{F}_7^7 \mid H\underline{v} = \underline{0} \right\}$.

a. Show that C_H is a subspace of $\mathbb{F}_7^7$. (5 points)

b. Show that C_H has weight 3. (7 points)

c. Let $\underline{v}' \in \mathbb{F}_7^7$. Show that $\left\{\underline{x} \in \mathbb{F}_7^7 \mid H\underline{x} = H\underline{v}'\right\}$ is the coset $C_H + \underline{v}'$. (5 points)

e. For $\underline{v}' = (1, 2, 3, 6, 0, 1, 2) \mod 7$ evaluate $H\underline{v}'$ and find the coset leader of the coset from part c. (5 points)

f. Find the $\underline{v} \in C_H$ which is closest in Hamming distance to the $\underline{v}'$ given in part e.; justify your answer. (3 points)

4 Reed-Solomon Codes (10 points)

Let $C_{\mathbf{RS}} \subset \mathbb{F}_7^7$ be the Reed-Solomon code obtained by evaluating polynomials of degree at most 3 at *all* 7 points of $\mathbb{F}_7$. Find the weight of $C_{\mathbf{RS}}$. How does this code compare with C_H?

5 Polynomials (15 points)

a. Calculate $\gcd(x^3 + x + [1]_3, x^2 + [2]_3)$ **in the ring of polynomials over** $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z}$. **(5 points)**

b. Show that there are no $f, g \in \mathbb{F}_3[x]$ **so that** $\left(\frac{f}{g}\right)^2 = x^2 + [2]_3$. **(10 points)**

6 RSA (15 points)

Bob advertises a public RSA key with modulus $m = 33$ and encoding exponent $e = 7$. You will play the role of Eve, the eavesdropper.

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 $[2]_{33}$, $[7]_{33}$ sent by Alice (7 pts).

7 Order of elements (10 points)

Let $(G, e, \cdot)$ be a group, and let $g \in G$.

a. Show that $\{n \in \mathbb{Z} \mid g^n = e\}$ is an ideal of $\mathbb{Z}$. (3 points)

b. Assume that $g^{37} = e$ but $g \neq e$. Show that $g^n = e$ if and only if $37|n$. (2 points)

c. Let $m \geq 1$ **and let** $a, b \in (\mathbb{Z}/m\mathbb{Z})^{\times}$ **have orders** r, s **respectively. Let** t **be the order of** ab**. Show: (5 points)**

$$\frac{rs}{(r,s)^2} \Big| t \qquad \textbf{and} \qquad t \Big| \frac{rs}{(r,s)} .$$