

# MATH/CSCI 2113

## Assignment 10

Due Monday, April 22.

1. Do problem 14.3.2 on page 651 of the text book.
2. In  $\mathbb{Z}_n$ , the integers modulo  $n$ , a *unit* is an element  $a$  so that there exists an element  $s$  so that  $a \cdot s \equiv 1 \pmod{n}$ . A (proper) *zero divisor* is an element so that  $ab \equiv 0 \pmod{n}$  for some element  $b$ , and neither  $a$  nor  $b$  are equivalent to zero modulo  $n$ . For example, 2 and 3 are zero divisors in  $\mathbb{Z}_6$ , and 5 is a unit in  $\mathbb{Z}_6$ . Find all the units and zero divisors in (a)  $\mathbb{Z}_{11}$ , (b)  $\mathbb{Z}_{12}$ , and (c)  $\mathbb{Z}_{10}$ .
3. (a) Give a proof of the following statement: If  $p$  is a prime, then  $\mathbb{Z}_p$  does not have a (proper) zero divisor.  
(b) Is the converse of the statement in (a) true? Give a proof or a counterexample.
4. Is the following statement true: If  $p$  is a prime, then the only unit in  $\mathbb{Z}_p$  is  $[1]$ . Give a proof or a counterexample.
5. Do problem 16.4.4 on page 719 of the text book.
6. Consider a binary code with code words of length  $n$ , and capable of correcting up to  $k$  errors.
  - (a) Let  $\mathbf{c}$  be a code word. How many different code words can be obtained from  $\mathbf{c}$  with exactly one bit in error?
  - (b) How many different codewords can be obtained from  $\mathbf{c}$  if *exactly*  $k$  bits are in error?
  - (c) How many different codewords can be obtained from  $\mathbf{c}$  if *at most*  $k$  bits are in error?
  - (d) Let  $m$  be the number of codewords in the code. Prove that the following inequality must hold:

$$m \left( \sum_{i=0}^k \binom{n}{i} \right) \leq 2^n.$$

(The bound above is called the *Hamming* bound.)

7. Describe all possible rectangle codes for code words of size 24. For each code, give the maximum number of errors it can correct, and give an example of the situation where one more error than allowed will lead to ambiguity, or to a wrong decoding.

8. Consider the Hamming code with four checks (this is a  $(15, 11)$  code).
- (a) Describe how the code works.
  - (b) Explain in detail how to decode the word 011100010111110. Is this a code word? If not, where is the error, and what is the correct message?