MATH/CSCI 2113

Assigment 10

Due Monday, April 22.

1. Prove that if a, b, c, n are integers with $a, n > 0$ and $b \equiv c \bmod n$, then $ab \equiv ac \bmod n$.

   Proof: Suppose a, b, c, n are integers with properties as in the statement. Since $b \equiv c \bmod n$, we know that $b - c = kn$ for some integer k. So $ab - ac = a(b - c) = akn$. Therefore, $ab - ac$ is a multiple of n, so $ab \equiv ac \bmod n$.

2. In $\mathbb{Z}_n$, the integers modulo n, a *unit* is an element a so that there exists an element s so that $a \cdot s \equiv 1 \bmod n$. A (proper) *zero divisor* is an element so that $ab \equiv 0 \bmod n$ for some element b, and neither a not 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) $\mathbb{Z}_{10}$.

   $\mathbb{Z}_{11}$: every element except 0 is a unit, and there an no proper zero divisors (this is true for every Z_p when p is prime.)

   $\mathbb{Z}_{12}$: 2,3,4,6,8,9,10 are proper zero divisors (for example, $6 \cdot 10 \equiv 0 \bmod 12$, so 6 and 10 are zero divisors).
   1,5,11 are the units. (for example $5 \cdot 5 \equiv 1 \bmod 12$.)

   $\mathbb{Z}_{10}$: 2,4,5,6,8 are proper zero divisors. 1,3,7 and 9 are units. ($3 \cdot 7 \equiv 1 \bmod 10$.)

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.

   (a) Proof by contradiction. Suppose p is a prime, and a is a proper zero divisor of $\mathbb{Z}_p$. Then there is an element b in $\mathbb{Z}_p$ so that $ab \equiv 0 \bmod p$, and neither a nor b is equivalent to 0 modulo p. So $p|ab$. Since p is a prime, this implies that $p|a$ or $p|b$ (see Chapter 4). But this implies that either a or b is zero modulo p, which is a contradiction.

   (b) Converse: if $\mathbb{Z}_p$ does not have a proper zero divisor, then p is prime. Proof by contrapositive. Contrapositive: if p is not prime, then $\mathbb{Z}_p$ has a proper zero

divisor. Suppose p is not prime. Then p is composite, so $p = ab$ for some integers a and b, where $1 < a < p$ and $1 < b < p$. So $ab \equiv 0 \bmod p$, but neither a nor b are equivalent modulo p. So a and b are proper zero divisors.

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.

   False. Every element in $\mathbb{Z}_p$ except 0 is a unit.

5. Do problem 16.4.4 on page 719 of the text book.

   (a) If at most two errors are made, the message will be decoded correctly. The probability that at most two errors are made is: $1 + 5(0.5)(0.95)^4 + \binom{5}{2}(0.5)^2(0.95)^3$.

   (b) We can now consider messages of length three as the "symbols" of the code. The probability that one or more errors occur in such a message equals: $p = 1 - (0.95)^3$. The probability that at most two of the length 3 messages are in error is: $1 + 5p(1-p) + \binom{5}{2}p^2(1-p)^3$.

   (c) In positions 1,3,5,7 and 9, we have 0,1,0,1,0. Majority equals 0. In positions 2,4,6,8,10, we have 1,1,0,0,1, majority is 1. So the word will be decoded as 01.

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.

   6×4: Can correct up to one error. The 4×6 rectangle will be expanded into a 5×7 rectangle, so code words have length 35. Example: 000000000000000000 will be encoded as $000 \ldots 0$ (35 zeros). If two errors occur in the first two positions, we get the following rectangle:

   $$\begin{array}{ccccccc} 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}$$

   None of the rows has parity check zero, while the first two columns have parity check zero. So it is impossible to find out in which row the two errors occurred. I.e. if the original words was 110000110000000000, and the errors occurred in positions 7 and 8, then exactly the same word would be received.

   3×8: Can correct up to one error. Code words have length $4 \times 9 = 36$.

   2×12: Can correct up to one error. Code words have length $3 \times 13 = 39$.

   1×12: Can correct up to one error. Code words have length $2 \times 13 = 39$.

8. Consider the Hamming code with four checks (this is a $(15, 11)$ code).
   (a) Describe how the code works.

   Form a parity matrix H of size 4×15, which has as its columns all bit strings of length 4:

   $$H = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

The code consists of all bit strings c of length 15 which have $Hc = 0$.

NOTE: the order of the columns may be different. This will affect your answer to problem (b). However, every possible ordering of the columns gives the same kind of code (same error-correcting capabilities, length etc. In fact, the codes can be obtained from each other as follows. For example, if C is the code obtained from the matrix H given above, and C' is the code obtained from the parity matrix H', which is equal to H except that columns 2 and 3 are switched, then C' can be obtained from C by switching the second and third bit of each word.

(b) Explain in detail how to decode the word $x = 011100010111110$. Is this a code word? If not, where is the error, and what is the correct message?

For the matrix H just given, $Hx = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix}$. This is equal to the third column. So an error occurred in the third position, and the correct codeword is 010100010111110.

Different answers possible, see note under (a).