Math 22, Review for Exam 2, Winter 2009

Here are some subjects, though not all…
Euclid. Alg
Linear congruences
RSA code implementation
Phi calculation
Prop. Logic question (truth tables, logical statements, etc.)
Predicate logic – universal and existential quantifiers ∀ and ∃
Proofs – various types
Codes – Hamming distance, error correcting codes
Codes – use of generator and check matrices
Graphs – counting vertices, edges and degrees/isomorphism
Graphs – Euler/Ham circuits
Graphs – Shortest path between vertices

(1) Euclidean Algorithm. (a) Show how to use the Euclidean Algorithm to find the greatest common divisor of 7 and 23.
(b) Find integers m and n such that 7m + 23n = GCD(7,23).

(2) Linear congruences. Solve $42x \equiv 36 \pmod{46}$ (hint: use the results from problem 1!)
$x \equiv$ _____ (show ALL solutions mod 46.)

(3) RSA code implementation. (a) Form an RSA coding scheme using the primes p=29 and q=31, and encoding key e=11. To encode the message "Z," we represent Z by the number 26 (since it is the 26th letter of the alphabet), and perform what operations? (Be specific - you need not actually perform the calculations.)

To encode: _____

(b) To decode the coded message in part (a), a (secret) decoding key must be found. What is the decoding key for the code above, and what operations must be performed to decode the message from part (a)? (Be specific - you need not actually perform the calculations.)

Decoding key = _____

(4) Phi calculation. $J = 2^n 3^m 11^k$, and there are 720 numbers from 1 to J that are relatively prime to J. Then J = _____

(5) Prop. Logic question (truth tables, logical statements, etc.) Construct a truth table for $p \wedge ((q \rightarrow r) \rightarrow p)$, and circle the column that represents your solution. (1 represents true, and 0 represents false.)

p	q	r	$(q \wedge (r \rightarrow p)) \vee r$
1	1	1	
1	1	0	
1	0	1	

1	0	0	
0	1	1	
0	1	0	
0	0	1	
0	0	0	

(6) Predicate logic – universal and existential quantifiers ∀ and ∃.

The Universal set is $Z^+ = \{1,2,3,...\}$.

(a) Express the negation of this proposition in formal symbols, and without using the word or symbol for "not" (you may use symbols for less then, greater than, less than or equal to, or greater than or equal to, as well as ∀ or ∃.)

$$(\forall k)\ (\exists n)(\forall m)\ kn \leq m$$

Answer: _____

(b) Which is true, the proposition in part (a), or its negation? _____

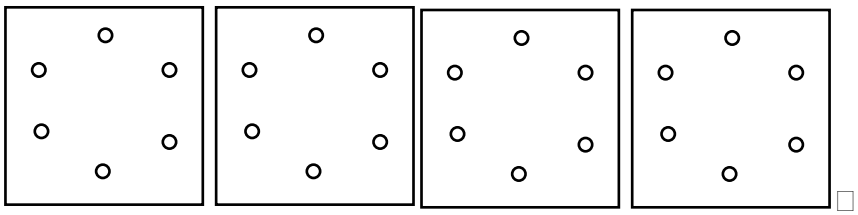
(7) Proofs – various types. For each of the following fill in the blank with the words *same as, converse of, inverse of,* or *contrapositive of*.

(a) The inverse of the converse of q->p is the _____ p->q.
(b) The contrapositive of the inverse of "p is necessary for q" is the _____ p->q.

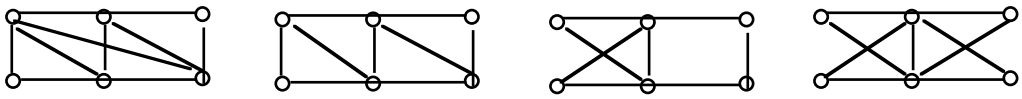
(8) Codes – Hamming distance, error correcting codes. Be able to find the Hamming distance between codewords; if a code's codewords all are at distance 12 or more from each other, then the code detects up to _____ errors, and corrects up to ____ errors.

(9) Codes – use of generator and check matrices. Given a generator matrix, be able to construct the check matrix and use it to check whether a purported code word is a code word or not. For example, number 17 in section 3.5. Also, be able to find the check matrix A* for the matrix A given in problem 17. Is (010101) a codeword for this code?

(10) Graphs – counting vertices, edges and degrees/isomorphism.
There are four non-isomorphic graphs (no loops or multiple edges) with six vertices and degrees 1,2,2,2,3, and 4. Draw them:



(11) Graphs – Euler/Ham circuits.



Write the letter(s) of any of these graphs which has a Hamiltonian Cycle and any that has an Euler Circuit:

____ has a Hamiltonian Cycle.

____ has an Euler Circuit.

(12) Graphs – Shortest path between vertices

List the vertices in the shortest path from S to K in this weighted graph:

_____