

Math 187 Test Four

Dr. Holmes

November 30, 2006

This exam begins at 1:40 pm and ends at 2:35 pm as usual. You may omit one question; if you do all questions your best work will be graded.

1. (makeup question for Test III) Give the multiplication table for mod 5 arithmetic.

Use the Euclidean algorithm to compute the multiplicative inverse of 7 mod 137. Be careful about minus signs.

2. Chinese Remainder Theorem: Determine the smallest solution to the system of equations

$$x = 11 \pmod{13}$$

$$x = 4 \pmod{17}$$

3. If my RSA key is $N = 187$ (you can factor this as $(11)(17)$ in spite of my fond imaginings otherwise) and my encryption exponent is $r = 3$, perform the following tasks.

Encrypt the message 13.

Determine my decryption exponent s .

For extra credit, you can decrypt the message 17 (I'll be impressed: the encryption exponent is not small).

4. Find $13^{64} \bmod 1000$.

- Two graphs are given. One has an Eulerian walk; one does not. For the one that does not, explain why it does not. For the one that does, exhibit the Eulerian walk as a list of vertices (arrows on the graph will not work!)

6. I remind you that Ore's theorem says that a graph has a Hamiltonian cycle if the degrees of any two vertices that are not adjacent add up to at least the number of vertices in the graph.

One of the following graphs does not satisfy the conditions of the theorem (and happens not to have a Hamiltonian cycle); explain why not. One of them does satisfy the conditions of the theorem and has a Hamiltonian cycle: exhibit the cycle as a list of vertices.

7. Three degree sequences are given. For each sequence, either draw a graph with that degree sequence or explain why there is no such graph.

8. A graph is given.

How many spanning subgraphs does this graph have? Draw a typical one (not the whole graph and not a tree).

How many induced subgraphs does this graph have? Draw a typical one with 5 vertices.

Draw a spanning subtree of this graph (with the same vertex labelling).

- Two graphs are given. Explain how the one on the left appears as a subgraph of the one on the right (you can do this by labelling the vertices of the graph on the right and labelling corresponding vertices in the graph on the left in the same way).