

Math 187 Test IV

Dr. Holmes

July 22, 2007

This exam begins at 8:40 am and ends at 9:35 am. You may use a plain scientific calculator with no graphing or symbolic computation. Cell phones must be turned off and out of sight.

1. (a) Use the Euclidean algorithm to find the greatest common denominator of 23 and 37, showing all work and clearly indicating to me that you know what the answer is: $\gcd(23, 37) = \dots$
- (b) Determine x and y such that $23x + 37y = 1$: this should come out of your gcd calculation. Show all work.
- (c) Determine the solution to the equation

$$23x \equiv 11 \pmod{37}$$

You should be able to use the previous work in this problem to do this problem fast. Your answer should be nonnegative and less than 37.

2. Write out the multiplication table for arithmetic mod 7.

3. Chinese Remainder Theorem: determine the smallest non-negative solution to the system of equations

$$x \equiv 3 \pmod{23}$$

$$x \equiv 14 \pmod{37}$$

4. If my RSA key is $143(= (11)(13))$ and my encryption exponent r is 7, perform the following tasks:
- (a) Determine my decryption exponent s .
 - (b) Encrypt the message 10.
 - (c) Set up the calculation I would need to do to decrypt the encrypted message you obtained as the answer to part b. For extra credit, you can carry out this calculation and verify that it does come out to 10 (don't do this unless you have finished the rest of the exam).

5. Euler's function and modular exponentation.

- (a) Compute $\phi(13)$, $\phi(169)$ and $\phi(60)$. Show all work.
- (b) Evaluate $7^{1000} \bmod 13$. This is very easy if you know how to use the Euler function to help simplify it.

6. Some degree sequences are given. For each sequence, either draw a picture of a graph with that sequence or explain why no graph can have that sequence.

(a) 1,1,1,2,2,5

(b) 1,1,2,3,4

(c) 2,2,2,2,2,2 (draw two non-isomorphic graphs with this degree sequence).

7. Two graphs are pictured. One has an Eulerian walk and the other does not. Explain why the one that does not have one does not have one, and give an Eulerian walk for the other one (as a list of vertices in the order that they are visited; just drawing arrows on the graph will not communicate anything to me).

- Two graphs are pictured. The left graph is isomorphic to a subgraph of the right graph, though it may not look as if this is true. Label the vertices of the graph on the left and label the corresponding vertices of the subgraph on the right in such a way as to show the isomorphism.

9. Explain why the number of vertices of odd degree in a finite graph must be even. We have shown this in class in two different ways: I don't expect the fancy induction argument, but the easier one that I gave first.