Math 189, Fall 2022, Test II

Dr Holmes

November 10, 2022

This exam will begin at 130 pm and end at 245 (officially). I will actually give a five minute warning at 245. You are allowed your test paper, your writing instrument, and a calculator without graphing or symbolic computation capability.

1. Number theory 1 Euclidean algorithm; find a modular reciprocal and solve a modular equation.

   The three tasks are all connected!

   (a) Find integers x and y such that $124x + 137y = \texttt{gcd}(124, 137)$. Show all work. This should include the usual table and should also make it clear that you know what x is, what y is and what $\texttt{gcd}(124, 137)$ is.

   (b) Find the reciprocal of 124 in mod 137 arithmetic.

   (c) Solve the equation $124z \equiv_{137} 5$ for z. Your answer should be a remainder mod 137.

2. Number theory 2 Chinese remainder theorem

   Solve the system of equations

   $x \equiv_{124} 112$

   $x \equiv_{137} 2$

   Give the smallest positive solution and the general solution.

3. Number theory 3 RSA problem

   In a comically absurd lack of awareness of the size of prime I need, I have chosen $p = 7, q = 13, r = 5$

   Describe my public RSA key and check that r has the required property.

   Compute my decryption exponent.

   Encrypt the message 15 to me, then decrypt it (since you can see right through my feeble attempts at security).

   A nibble of extra credit: my favorite message is 42, and encrypting and decrypting it with this key did work. But I didn't want to do it. Can you see why (there is something wrong with it with this key!)

4. Number theory 4 Prove Euclid's Lemma: if a, b are integers and p is a prime, and $p|ab$, then either $p|a$ or $p|b$. Your proof will use the extended Euclidean algorithm theorem.

5. Graph theory 1 Definitions

   Do two of the three parts. If you work on all three your best work will count and you may get extra credit.

   (a) Prove (the explanation is fairly brief) that a finite graph must have an even number of vertices of odd degree.

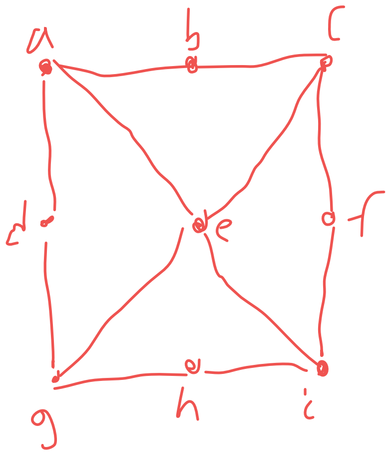
   (b) Prove (this can be a quite brief explanation) that the degrees of the vertices in a finite graph with at least two vertices cannot all be different.

(c) For each of the following degree sequences, draw a graph with that degree sequence or explain why there can be no such graph.

   i. 1,2,2,3,3
   ii. 3,3,3,3
   iii. 3,3,3,3,3,3,6 (this one is possible: draw two non-isomorphic graphs with this degree sequence) Hint: this is a slight modification of the example in the practice exam.

6. Graph theory 2

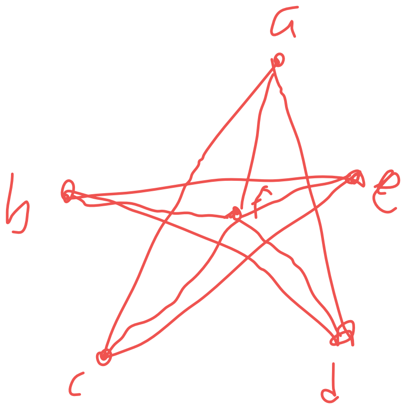
(a) Find a spanning tree of the given graph. Draw a separate picture of the spanning tree, and then color the vertices of the spanning tree using two colors (with the expected rule for colorings).



(b) Show me a connected graph in which every vertex is of degree 2 or less which cannot be colored with two colors. Explain why it cannot be colored with two colors.

7. Graph theory 3 Planar graphs

(a) Show that the pictured graph is planar by giving a different picture of it. Color it with four colors. Explain why you cannot color it with three.



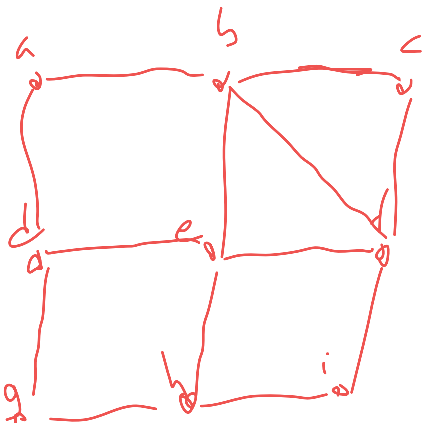
(b) A planar graph has six vertices and divides the plane into four regions (including the outside); how many edges does it have? Draw a graph like this which contains a six-cycle. Draw another graph like this which does not contain a six-cycle.

(c) Substantial extra credit: prove using Euler's formula that the complete graph with 5 vertices is not planar.

8. Graph theory 4 Eulerian walks and trails

Two graphs are pictured. In one there is an Eulerian walk (a walk which visits each edge in the graph exactly once); in the other there is not. Present the walk in the graph which has one as a sequence of vertices (vertices can be repeated, of course); explain briefly why the graph which does not have one cannot have one.

A



B