Math 189, Fall 2022, Test II (practice version)

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 $111x + 137y = \texttt{gcd}(111, 137)$. 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 $\texttt{gcd}(111, 137)$ is.

   Output from my spreadsheet embedded.

```
a= 137 1 0 137
b= 111 0 1 138
26 1 -1 1 136
7 -4 5 4 142
5 13 -16 3 121
2 -17 21 1 158
1 47 -58 2 79
```

   $(47)(137) + (-58)(111) = 1 = \texttt{gcd}(111, 137)$

   (b) Find the reciprocal of 111 in mod 137 arithmetic. 137-58 = 79.

   (c) Solve the equation $111z \equiv_{137} 4$ for z. Your answer should be a remainder mod 137.

multiply both sides by $79 = 111^{-1} \texttt{mod} 137$ to get $x \equiv_{137} (4)(79) \equiv_{137} 42$. That was not intentional.

2. Number theory 2 Chinese remainder theorem

Solve the system of equations

$x \equiv_{111} 25$

$x \equiv_{137} 124$

Give the smallest positive solution and the general solution.

$x = 124 + 137k$ for some k.

So $124 + 137k \equiv_{111} 25$ which simplifies to $13 + 26k \equiv_{111} 25$ or $26k \equiv_{111} 12$.

```
111 1 0
26 0 1
7 1 -4 4
5 -3 13 3
2 4 -17 1
1 -11 47 2
```

$26^{-1}\texttt{mod}111 = 47$

so $k \equiv_{111} (12)(47) \equiv_{111} 9$

so $x = 124 + 137k = 124 + (137)(9) = 1357$

The smallest positive solution is 1357 and the general solution is $1357 + 15207n$ where n ranges over all integers. $15207 = (111)(137)$

3. Number theory 3 RSA problem

   In a comically absurd lack of awareness of the size of prime I need, I have chosen $p = 7, q = 19, r = 5$

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

   $N = (7)(19) = 133$

   $(p-1)(q-1) = 6 * 18 = 108$

   5 is relatively prime to 108, so meets the requirement to be r.

   Compute my encryption exponent.

```
a= 108 1 0 108
b= 5 0 1 109
3 1 -21 21 87
2 -1 22 1 130
1 2 -43 1 65
```

   The encryption exponent is $5^{-1}\mathtt{mod}108 = 65$

   Encrypt the message 32 to me, then decrypt it (since you can see right through my feeble attempts at security).

   Compute $32^5\mathtt{mod}133$ to encrypt.

   Encryption taken from the spreadsheet doesnt format very well in Latex, but should give something to check your calculations against, or inspire you to use the spreadsheet.

```
133 <---modulus

32 <----base of exponentation
5 <---exponent
5 1 128 4 128
2 0 93 93 93
1 1 32 1 32
0 0 1 1 1
```

   The encrypted message is 128.

   To decrypt, compute $128^{65}\mathtt{mod}133$.

```
133 <---modulus

128 <----base of exponentation
65 <---exponent
65 1 32 100 32
32 0 123 123 123
16 0 16 16 16
8 0 4 4 4
4 0 93 93 93
2 0 25 25 25
1 1 128 1 128
```

It decodes back to 32.

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!)

The problem is that 42 has a common factor 7 with 133. But in fact it encrypts and decrypts just fine.

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.

   Suppose that a, b are integers and p is prime.

   Either p goes into a (case 1) or it doesn't (case 2).

   In case 1 we have $p|a$ so we have $p|a$ or $p|b$.

   In case 2, we have $p \not| a$ so $\texttt{gcd}(p, a) = 1$

   Thus, by the extended Euclidean algorithm, there are integers x, y such that $px + ay = 1$.

   Now $b = b1 = b(px+ay) = bpx+bay$. bpx is divisible by p by inspection. bay is divisible by p because $p|ab$.

   Thus p goes into $bpx + bay = b$. Since we have $p|b$ we have $p|a$ or $p|b$.

   So $p|a$ or $p|b$ follows in both cases.

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 (this is really a brief explanation) that the total degrees of the vertices in a graph must be even.

Each edge contributes 1 to the degree of exactly two vertices, so contributes 2 to the sum of all the degrees, which is thus twice the number of edges and so even.

(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.

Suppose G has n vertices. There are n possible degrees for vertices in G, the integers from 0 to $n-1$ inclusive. For all the vertices in G to have different degrees, all the possible degrees must actually occur as degrees of vertices in G, but G cannot have vertices of degree both 0 (connected to no other vertex) and $n-1$ (connected to all other vertices). So there cannot be such a graph.

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

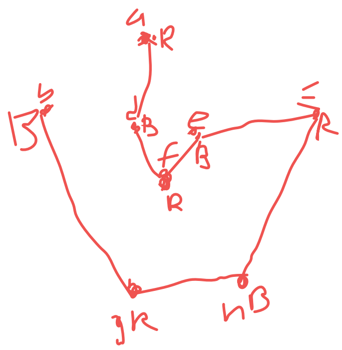
i. 1,1,2,3,4 impossible, sum of degrees odd

ii. 1,2,2,3,4 picture

iii. 2,2,2,2,2,2 (this one is possible: draw two non-isomorphic graphs with this degree sequence) picture

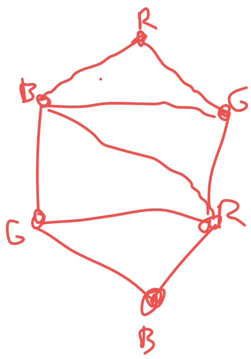
6. Graph theory 2

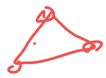
(a) Find a spanning tree of the given graph. Draw a separate picture of the spanning tree, and then color the vertices of the spanning tree using two colors (with the expected rule for colorings).



One of many possible sols

(b) Color the pictured graph with three colors. Explain briefly why you cannot color it with two colors.

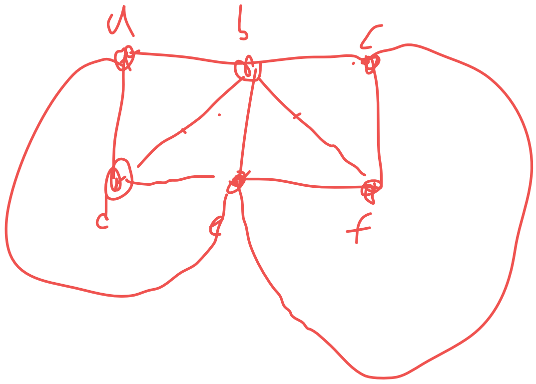


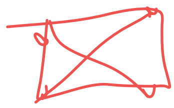


needs
3 colors

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.



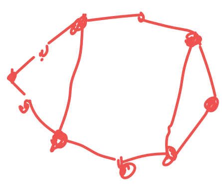


K_4 needs 4, it has K_4 subgraph

(b) A planar graph has ten vertices and divides the plane into four regions (including the outside); how many edges does it have?

$V - E + F = 2$, that is $10 - E + 4 = 2$, so $E = 12$

Draw a graph like this. picture



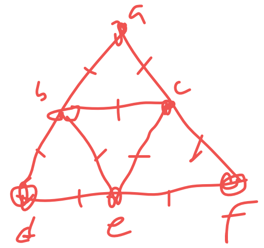
(c) Substantial extra credit: prove using Euler's formula that the complete graph with 5 vertices is not planar.

Its in the book or the notes.

8. Graph theory 4 Eulerian walks and trails

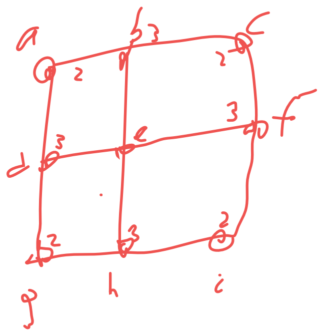
Two graphs are pictured. In one there is an Eulerian walk (a walk which visits each edge in the graph exactly once); in the other there is not. Present the walk in the graph which has one as a sequence of vertices (vertices can be repeated, of course); explain briefly why the graph which does not have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

A



a, c, f, e, c, b, e, d, b, a

B



4 vertices of odd degree impossible