Final examination, Math 305, spring 2022 (take home bits)

Randall Holmes

April 24, 2022

There are five questions. Don't miss the next page.

This is due at 11:55 pm Friday May 6. Please turn it in electronically to me. You are not allowed to consult any other person but me.

Please note that problem 4 involves separate communications from me. These will be sent out on Sunday, May 31. If you request them earlier they can be sent earlier.

I do not commit myself as to how much this may count; I'll make a decision about that when I see how everything looks.

1. Show full hand calculations for encryption of 111 using the RSA key $(137)(211) = 28907$ and decryption of the result back to 111 (so you need to find the decryption exponent). I'm counting this as a full workout on modular arithmetic. Of course you can use my tools to set up your calculation, but show on your paper what manual calculation would look like.

2. Work out the multiplication table for D_5, the group of symmetries of a pentagon (these groups are discussed in the book).

   Write cycle notation for each element of the group as a permutation of the vertices of the pentagon.

   List the subgroups. For each one, determine its left and right cosets.

   Identify the subgroups which are normal and the subgroups which are not.

3. Exhibit two different isomorphisms between $\mathbb{Z}_{15}$ and $\mathbb{Z}_3 \times \mathbb{Z}_5$, as tables of values of a finite function. How many isomorphisms are there? (elements of $\mathbb{Z}_3 \times \mathbb{Z}_5$ are pairs of numbers like (2,3)).

   Give a convincing argument that $\mathbb{Z}_2 \times \mathbb{Z}_4$ is not cyclic (and so not isomorphic to $\mathbb{Z}_8$). This should use simple facts about the group, not Theorems.

4. Under separate cover (individual email) I will send you an RSA key and an El Gamal key, at the end of dead week. Encrypt a message (your student ID number) with each key and mail it back to me. If I can successfully decrypt it, you have credit.

5. Find all the Rabin-Miller misleaders for 25. Show the calculations (of course, use my spreadsheet or Python functions to find them!)