Final Project Guidelines

Math 335

The final project for Math 335 will be a mini research project, in which you undertake a guided exploration of a topic related to the material of our course, learn about some relevant ideas through reading, and then create a report on your findings. This is meant to simulate the process of mathematics research, to help you see whether that might be something you're interested in pursuing further (for example, via the Master's program at San Francisco State).

Project Structure: The first step toward the final project is to choose a topic from the list of five possibilities at the end of this document. Once you've chosen your topic, the process of completing the project will consist of three main components:

- answering a series of open-ended exploration problems;
- reading a short excerpt from the Gallian textbook on a concept related to the exploration problems you've been tackling;
- creating a report that discusses both the findings from your exploration problems and the content of your reading, and how they relate to one another.

The first two components will be included on homework assignments, beginning immediately after the second exam.

Report Deadline: The final report is due on **Thursday, May 20**, via iLearn.

Report Format: The final report can be in the form of a paper (in which case it should be typed and be approximately three pages in length) or a video presentation (in which case it should be approximately ten minutes in length). Your goal is to explain what you learned in a way that would be understandable to a member of our class who did not study the same topic as you. There will likely be a number of other members of the class all working on the same topic, and I encourage you to discuss what you're learning with them; however, the final report should be created individually.

Grading: Your final report will be graded based on the following components:

- **Completeness**: Discuss both the exploration problems and the reading in a way that responds to the prompts on the topic list.
- **Correctness**: Explain the results of your explorations, as well as any definitions or theorems from your reading, in a correct and mathematically rigorous way.
- **Exposition**: Tie together your explorations and your reading into a coherent narrative. Express yourself in your own words, in language that would be understandable to a member of our class who hasn't learned about your topic.
- **Polish**: Put together a neat typed document without typos, or a well-rehearsed video presentation with both speaking and visual aids.

Topic List

I encourage you to glance at the reading for a topic to help you decide whether you're interested in it. (You can can also glance at the exploration problems, which are on the following pages of this document.) However, to avoid spoiling the fun of the exploration problems, it would be best not to look too closely at the readings just yet!

Topic #1: Even/odd permutations and the alternating group

- **Prompt**: Can an element of S_n necessarily be expressed as a composition of transpositions? To what extent is this expression unique? What can we say about the number of transpositions involved in this expression?
- **Reading**: Gallian, Chapter 5 (pages 108–111)

Topic #2: Symmetries and the orbit-stabilizer theorem

- **Prompt**: How many rotational symmetries does a three-dimensional shape have? How can we calculate this number in a systematic way?
- **Reading**: Gallian, Chapter 7 (pages 151–153)

Topic #3: The group of units modulo n

- **Prompt**: Which elements of $\mathbb{Z}_n$ have inverses under multiplication? What is the relationship between the elements with multiplicative inverses in the groups $\mathbb{Z}_n$, $\mathbb{Z}_m$, and $\mathbb{Z}_{nm}$? And (optionally) how is all this related to cryptography?
- **Reading**: Gallian, Chapter 2 (Example 11) and Chapter 8 (pages 166–168 and optionally, pages 168–172)

Topic #4: Existence of subgroups of given order

- **Prompt**: We know that the order of an element in G (as well as the size of a subgroup of G) divides $|G|$, but what about the converse? In other words, if d divides $|G|$, does there exist an element in G of order d? How about a subgroup of G with d elements?
- **Reading**: Gallian, Chapter 24 (pages 409–414)

Topic #5: The Euler ϕ-function

- **Prompt**: Given a group G and an integer d dividing $|G|$, how many elements does G have of order d? Can we answer this question when $G = \mathbb{Z}_n$? How about for other groups G?
- **Reading**: Gallian, Chapter 4 (pages 84–85)

Exploration Problems for Topic #1

No need to start working on these right away; they'll be assigned on Homeworks 8, 9, and 10.

EP1. Recall from Homework 3 that a *transposition* is defined as an element of S_n that swaps two numbers but sends every other number to itself. The guiding question of this problem is: can every element of S_n be expressed as a composition of transpositions?

(a) Choose a few specific elements of S_n and express them as compositions of transpositions. (You've done some of this already on Homework 3, but make up some other examples besides the ones included there.)

(b) Suppose that

$$f = (a_1\ a_2\ a_3\ a_4) \in S_n$$

is a cycle of length 4. (For instance, on Homework 3, you considered the cycle $f = (1, 2, 3, 4) \in S_4$.) Can you find a general formula in terms of a_1, a_2, a_3, a_4 for how to express f as a composition of transpositions?

(c) Generalize your recipe from part (b) to give a formula for expressing any cycle

$$f = (a_1\ a_2\ a_3\ \cdots\ a_d) \in S_n$$

as a composition of transpositions.

EP2. What you did in EP1 shows that any element of S_n can be expressed as a composition of transpositions. The guiding question of this problem is: is this expression unique?

(a) Choose a specific element of S_n, and write it in two different ways as a composition of transpositions.

(b) Choose an element of S_n that you know you can express as a composition of two transpositions (like, for example, $(1, 2)(2, 3)$ in S_3). Can you express that same element as a composition of more than two transpositions?

EP3. This problem builds on EP2, focusing specifically on the identity element $e \in S_n$.

(a) Express $e \in S_4$ as a composition of transpositions.

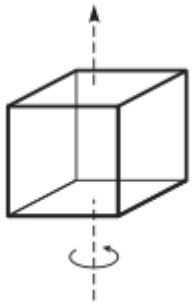
(b) Can you express $e \in S_4$ as a composition of two transpositions? Three transpositions? Four transpositions?

(c) Suppose that I tell you I've expressed $e \in S_n$ as a composition of r transpositions. Based on your findings from part (b), make a guess about what you can say about the number r.

Exploration Problems for Topic #2

No need to start working on these right away; they'll be assigned on Homeworks 8, 9, and 10.

EP1. A *rotational symmetry* of a three-dimensional shape P is a rotation of 3d space that takes each point in P to another point in P. For instance, a cube has a rotational symmetry given by rotating by 90° around the axis shown below:



(a) How many rotational symmetries does a cube have? Try to list them all systematically.

(b) How many rotational symmetries does a tetrahedron (a pyramid with four sides, each of which is an equilateral triangle) have? Try to list them all systematically.

EP2. Let P be a polyhedron (a 3d shape like a cube or tetrahedron) and let f be a face of P (meaning one of its sides, like the six sides of the cube or the four sides of the tetrahedron). The *stabilizer* of f is defined to be the set

$$\text{stab}(f) = \{\text{rotational symmetries that keep } f \text{ where it is.}\}.$$

For example, if f is the top side of the cube shown in the above picture, then the 90° rotation around the axis shown is a rotational symmetry that keeps f where it is.

(a) Pick any face f of a cube. How many elements does $\text{stab}(f)$ have?

(b) Pick any face g of a tetrahedron. How many elements does $\text{stab}(g)$ have?

EP3. What seems to be the relationship between the answers to EP1 and EP2—in other words, between the number of rotational symmetries of a shape and the number of elements in the stabilizer of a particular face? If you have a guess, test it on a different shape, like the octahedron or dodecahedron. (You can look up online what these other shapes look like.)

Exploration Problems for Topic #3

No need to start working on these right away; they'll be assigned on Homeworks 8, 9, and 10.

EP1. Let

$$U(n) \subseteq \mathbb{Z}_n$$

be the set of elements in $\mathbb{Z}_n$ that have inverses under the operation of **multiplication** modulo n. (For instance, $3 \in U(4)$ because 3 has an inverse under the operation of multiplication modulo 4.)

(a) For each $n \in \{2, 3, 4, \ldots, 10\}$, find all the elements of $U(n)$.

(b) Make a table that shows, for each $n \in \{2, 3, 4, \ldots, 10\}$, the number of elements in $U(n)$. Do you have any observations about this table?

EP2. Based on your data from EP1, does it seem to be true that

$$\Big|U(nm)\Big| = \Big|U(n)\Big| + \Big|U(m)\Big|?$$

Is this true for some values of n and m? If so, can you make a guess about when it's true?

EP3. Try to define a function

$$\phi : U(nm) \to U(n) \oplus U(m)$$
$$\phi(a) = (a \mod n,\ a \mod m).$$

For instance, if $n = 3$ and $m = 4$, then

$$\phi : U(12) \to U(3) \oplus U(4)$$

sends

$$\phi(5) = (5 \mod 3,\ 5 \mod 4) = (2, 1)$$

(a) When $n = 3$ and $m = 4$, write out what ϕ does to each element of $U(12)$. Is ϕ a bijection in this case?

(b) Now try taking taking $n = 3$ and $m = 6$, and writing out what ϕ does to each element of $U(18)$. Does anything go wrong? If so, what?

Exploration Problems for Topic #4

No need to start working on these right away; they'll be assigned on Homeworks 8, 9, and 10.

EP1. Let G be a group with 8 elements. We know that the order of any element of G must be a divisor of 8, but the guiding question of this exploration problem is: does there necessarily exist an element of each of these orders?

(a) Does G necessarily have an element of order 1? If so, explain how you know. If not, give a specific example of a group G with 8 elements that doesn't have an element of order 1.

(b) Does G necessarily have an element of order 2? If so, explain how you know. If not, give a specific example of a group G with 8 elements that doesn't have an element of order 2.

(c) Repeat what you did in parts (a) and (b) for order 4, and order 8.

EP2. Again, let G be a group with 8 elements. A closely related issue to what you considered in EP1 is the size of subgroups of G. In particular, we know that the size of any subgroup of G must be a divisor of 8, but in this problem, we ask: does there necessarily exist a subgroup of each of these sizes?

(a) For which divisors d of 8 can you definitively say that G has a subgroup with d elements?

(b) Do you think that G has a subgroup with d elements for *any* divisor d of 8? You don't have to prove your answer, but back it up by considering some specific groups with 8 elements.

EP3. Let G be the following subgroup of the symmetric group S_4:

$$G = \{e,\ (1,2,3),\ (1,3,2),\ (1,2,4),\ (1,4,2),\ (1,3,4),\ (1,4,3),\ (2,3,4),\ (2,4,3),\\ (1,2)(3,4),\ (1,3)(2,4),\ (1,4)(2,3)\}$$

(In other words, G consists of the identity element, all cycles of length 3, and all compositions of two disjoint cycles of length 2.) This G is a group with 12 elements, and it's special in that it *doesn't* have subgroups of every size dividing 12. Test this out: can you find a subgroup of G with 1 element? With 2 elements? 3? 4? 6? 12?

Exploration Problems for Topic #5

No need to start working on these right away; they'll be assigned on Homeworks 8, 9, and 10.

EP1. The guiding question of this problem is: how many elements of order d does $\mathbb{Z}_n$ have? (Throughout, we're thinking of $\mathbb{Z}_n$ as a group under the operation of addition modulo n.)

(a) Choose a specific value of n, and then, for each divisor d of n, count how many elements $\mathbb{Z}_n$ has of order d.

(b) Repeat part (a) for a different value of n.

(c) If I choose an element of $\mathbb{Z}_n$, is there a quick way to tell whether it has order n? How about whether it has order d for some other divisor d of n?

EP2. In EP1, you considered the question "how many elements of order d does $\mathbb{Z}_n$ have?" The guiding question in this problem is: does the answer to the above question depend on n?

(a) Count how many elements of order 3 there are in $\mathbb{Z}_6$, and then how many elements of order 3 there are in $\mathbb{Z}_9$.

(b) Do you think that the answer to the question "how many elements of order d does $\mathbb{Z}_n$ have?" depends on n? You don't have to prove your answer, but back it up with some examples or explanation.

EP3. For any positive integer d, let $\phi(d)$ be the number of elements of order d in $\mathbb{Z}_d$. (Based on the observations of EP2, this is the same thing as the number of elements of order d in $\mathbb{Z}_n$ for any n that's a multiple of d.)

(a) Calculate $\phi(d)$ for each $d \in \{2, 3, 4, 5, 6, 7, 8, 9, 10\}$, and arrange your calculations into a table.

(b) Do you have any observations about the table in part (b)?