A Helpful Handout for your Projects

Your final projects are due the day of our exam.

1. The Written Projects

The written parts can take on many forms (e.g., a collection of worked out problems, a biography, a survey of a particular theorem, etc) but I expect most of you will be writing some kind of paper. If you're doing something other than writing a paper and you'd like a guide like what follows, let me know and I will try to provide you with one.

If you are writing a paper, here's what I'll be looking for, generally:

- Have presented ideas in a logical order?
- Is your essay written in clear, grammatically correct prose?
- Have you offered explanation or examples to support generalizations?

Each of these general categories break down into more detail:

- IDEAS
  - Do you understand the big ideas and context behind what you're writing about?
  - Do you offer original interpretations?
  - Do your explanations of terms, ideas, and examples demonstrate an ability to grasp the main points, paraphrase them, and apply them?
  - Does your essay demonstrate an understanding of a subject, or does it wander from one subject to the next without offering more than superficial remarks?
- ARGUMENT
  - Can I easily determine what your main point is (even though it's about math, it should still have a main point)?
  - Does your essay provide a series of points that add up to an argument supporting the main point (thesis)?
  - Does your essay proceed logically from point to point?
  - Do you provide examples and explanations to support his or her generalizations?
  - Does your essay contain contradictions? Is the paragraph structure logical?
- MECHANICS AND STYLE
  - Do you control tone? Is the essay free of grammatical errors?
  - Is your essay punctuated appropriately?
  - Do citations and bibliography follow some format (e.g., the MLA)?
  - Is the prose clear or will I puzzle over individual sentences?
  - Are words spelled correctly?

2. The Status Reports

Learning how to present mathematics to an audience is a challenging task. I've been doing it for a while, and I'm still not that good at it. For your oral presentation, there are two different approaches: you could give a board talk or a power point presentation. In both cases, there are some general principles to which you want to adhere:

- Your talk should last a total of 3 to 5 minutes (I may cut you off).
- You should be an expert on the topic you chose:
  - Don't be afraid to be technical, where appropriate.
  - Your audience is your fellow students — you should be familiar with their background.
  - Refresh their memory but don't insult their intelligence.
- Your talk should be polished.
  - Consider distributing a short handout.
  - Practice!
- Here things not to do (if you're using the board):

  - Not envisioning the board as having distinct parts (e.g., your writing goes all the way across the board)
  - Not facing the audience
  - Being careless or lazy with your handwriting
  - Not pausing between sentences.
  - Making weird choices about what to write on the board and what not to write (e.g, maybe you say the definition out loud and then work an example out on the board).

3. Suggested Topics

- General stuff
  - An introduction to Fermat's Last Theorem
  - Public-key cryptography
  - RSA
  - Discrete Log problem and ElGamal
  - The AKS algorithm
- CS-ish
  - Computing in $\mathbf{Z}/p\mathbf{Z}$
  - Factoring today
  - Elliptic curve cryptography
  - Shanks's point counting algorithm (baby step/giant step) – solving the discrete log problem
  - Schoof's algorithm (counting points on a curve mod a prime)
  - Why use Elliptic curves for crypto?
- Mathy
  - Matijasevich's theorem
  - Elliptic curves over $\mathbf{Z}/p\mathbf{Z}$ and Hasse's Theorem
  - Elliptic curves of large rank and the distributions of rank
  - Elliptic functions: why they're called elliptic curves
  - Elliptic curves over $\mathbf{C}$: why are ECs donuts?
  - Pendulums, elliptic functions and elliptic curves
  - Bezout's theorem
  - Lentra's elliptic curve factoring algorithm
  - Taxicab and Cabtaxi numbers