1 Final Paper

Your final assignment in 18.704 will be an expository paper. You should aim for around 10 pages or so in length. The official due date is Wednesday Dec. 8, since this is our last day of classs. You should think of this as a firm deadline, to help pace yourself, and because you don't want it hanging over your head during finals week. If necessary there can be a little flexibility there though.

You should aim to pick a topic soon, either from this list or not, and discuss it with me by next week. If you pick your own, it should at least fall into the general areas of number theory or algebraic geometry. Set up an appointment or just stop by. By far the longest part of writing this paper should be reading the sources you will use and gaining a general understanding of them, and figuring out what you want to include. That part should not be left until the last minute. The writing part is not meant to take you nearly as long. I'm generally suggesting topics that I don't know all of the details about myself. Your job is to teach me something about the topic, assuming I know about as much basic background material as you do.

The things I hope you gain from this experience are (1) learning something new you hopefully find interesting, and (2) practice summarizing the main ideas of some topic in mathematics. Some of the topics below are a bit more advanced than the material in our book, and you shouldn't necessarily feel that you have to understand every detail of what you read; in any case you won't have enough space to give all of the details in your paper, and needn't expect to give proofs of everything you state.

If you know LaTeX, I'd love if you use it to write your paper. If you don't, this might be a great opportunity for you to learn it; you really only have to write one paper using it to get a basic knowledge, and then you'll have it at your disposal for the future. But I'm also perfectly happy with neatly hand-written papers.

The books mentioned below I have in my office for you to peruse or make photocopies or borrow for the evening whenever you want (mostly they're library copies; I took them out myself rather than put them on reserve.)

2 Possible Topics

These topics are probably too big and general; if you see something you like, come chat with me about it and we'll see how best to cut it down to the right size. If you have no idea what to pick or don't like any of these at all, come see me so we can discuss options.

(1) Rational points on Conics over $\mathbb{Q}$. The text shows how to find all rational points on a conic in Section I.1, provided you know that the conic *has* a rational point. To decide if a rational conic has a rational point, there is a theorem of Legendre, or a more general version by Hasse. Describe some of the results in this area with some proofs. Possibility 1: describe Legendre's fairly elementary

solution to this problem, maybe also mentioning Hensel's Lemma. See [NZM], Section 5.5. Possibility 2: describe the more general version due to Hasse. This requires you to learn some preliminaries on p-adic numbers, and you won't have space to present all of the details of the proof. See [Cas], Chapters 1-5.

(2) Integer points on Conics over $\mathbb{Q}$. For some special kinds of conics, the integer points can be found exactly. For example, you might study the solution to Pell's equation (you should do this topic only if you haven't already seen this material), summarizing first some basic properties of continued fractions. A basic reference is [NZM], Chapter 7.

(3) Proof of a special case of Fermat's last theorem. (For people with an abstract algebra background but who have not taken algebraic number theory.) Learn a bit about algebraic number theory, enough to understand units and unique factorization in number fields. Summarize the main ideas and use them to prove Fermat's last theorem for the case of a regular exponent p, i.e. there are no integer points on the curve $x^p + y^p = z^p$ unless one of x, y, z is 0, where p is a so called regular prime. Or even just concentrate on the case $p = 3$. A basic reference is [NZM], Chapter 9, or [Poor], Chapter 1-4.

(4) Elliptic curves and cryptography. Investigate some elements of this subject beyond what is in Section IV.4 of our book (which describes how elliptic curves are useful to help factor large integers.) Possibilities are: how elliptic curves are used for primality testing, or how elliptic curves are used to actually create codes, possibly including the discrete logarithm problem for elliptic curves. References include [Wash] Chapters 5,6, [BNRV] part III, or [Ko1] Chapter 6.

(5) Fermat's last theorem, a more historical approach. Discuss a bit of the history of Fermat's last theorem, what methods were used to attack it in the past, together with a necessarily *very* superficial discussion of the method used in Andrew Wiles' eventual proof from the 90's. You might consider merging the material discussed in one of the "math books for nonmathematicians" which describe Fermat's last theorem, (for example [Azcel], though there are many others), with a wee bit culled from an advanced summary of Wiles' proof, for example the one in [CSS] Chapter 1 (a lot of this will seem impossible to understand, but try to tease out the main ideas.)

(6) The congruent number problem. Describe this interesting number-theoretic problem and how it is related to the theory of elliptic curves (this probably requires mentioning L-functions and the Birch-Swinnerton-Dyer conjecture.) Reference: [Ko2] especically chapter 1.

I'm less sure about the feasibility of the next two. But if they are examples of slightly more advanced kinds of topics you could consider if you know more background in some particular subject.

(7) Defining the group law using divisors (for someone ambitious with some background in algebraic geometry). Describe a little bit of the theory of divisors on curves, and use it to show that an elliptic curve gets a natural group law by using its divisor class group. This shows how the ugly proof of associativity we used in class can be avoided. See [S] Sections III.1 through III.3.

(8) Complex tori (for someone ambitious with a background in complex analysis). Describe more details of the correspondence between elliptic curves and the complex plane modulo a lattice which we studied in Section II.2 of the book. For example see [A] Chapter 7 or [Hus] Chapter 9.

References

[Hus] Dale Husemoller, *Elliptic Curves.*

[A] Lars Ahlfors, *Complex Analysis.*

[CSS] Cornell, Silverman, and Stevens, *Modular Forms and Fermat's Last Theorem*

[Cas] Cassels, *Lectures on Elliptic Curves*

[Azcel] Amir Azcel, *Fermat's Last Theorem*

[BNRV] Bhandari, Nagraj, Ramakrishnan, and Venkataramana, *Elliptic Curves, Modular Forms and Cryptography*

[Wash] Lawrence Washington, *Elliptic Curves: Number Theory and Cryptography*

[NZM] Niven, Zuckerman, and Montgomery, *An introduction to the Theory of Numbers*

[S] Shafarevich, *Basic Algebraic Geometry I*

[ES] Erdos and Suranyi, *Topics in the theory of numbers*

[Ko1] Neal Koblitz, *A course in Number Theory and Cryptography*

[Ko2] Neal Koblitz, *An Introduction to Elliptic Curves and Modular Forms*

[Poor] Alf van der Poorten, *Notes on Fermat's last theorem*