Paper Topics
Due: May 9, 2019

You are expected to write a 4–6 page paper, in LaTeX, on the topic you have chosen. The paper should contain a clear statement of a significant result or idea that you are presenting, a little motivation or history, relevant definitions, and mathematical work. The latter should include a significant proof, worked-out examples, data gathered from numerical experiments, and/or algorithms; proofs are best, of course! The amount of actual mathematical work should be equivalent to roughly two or more homework assignments. Completed papers will be posted on my webpage so that your classmates can read them. As the intended audience is your classmates, you can assume anything covered in class.

Dates. You must choose a topic by **March 1**. An outline is due **March 21**. A first version is due on **April 25**. The revision is due **May 9**, and should be turned in *both* as a hard copy and emailed to me as a pdf.

Grading. The grading for the final paper is as follows:

5%	for outline
10%	for first version
30%	for completing the assignment as instructed
35%	for correct and substantive mathematics
10%	for clear, organized writing
10%	for correct spelling, grammar, and LaTeX

The outline should clearly state the main theorem or other result of your paper, a roadmap for proving it, and an idea of what other material is in the paper (if any).

The grading for the first version is meant to reflect the final grade, so if you turn in the first version without changes, that grade will essentially stand. For example, if you get a 10 on the first version and then hand it in again without changes, you'll get between a 95 and 100 for your final paper grade.

Format. To typeset your paper, you **must** use LaTeX! Use the article document class without a font specification. The bibliography does not count towards page limits. The intended audience is your classmates, so you should assume knowledge of anything in this course or its prerequisites without citation. I strongly encourage you to use the template I have provided on my webpage. For your bibliography, you may not use online sources unless they are print documents (e.g. pdf) found online.

As for length, I don't particularly care about the final page count. For me, the important thing is the mathematical content. That means that if a sentence could safely be deleted without much impact on the mathematical content of your paper, please do so, even if it brings your paper to fewer than 4 pages!

Plagiarism. I take plagiarism seriously, and you should too! Plagiarism is *not* just copying; rephrasing or paraphrasing counts as well. For example, if the original source said

> The difference between Euclidean and affine geometry stems from the smaller group of isometries in the former. Specifically, affine isometries include nonsingular linear transformations, which do not necessarily preserve distance nor angles.

then the following would constitute plagiarism:

> Euclidean geometry has fewer isometries than affine geometry. This is because invertible linear transformations are isometries for affine space but not for Euclidean space. Note that these transformations don't have to keep distance or angle measure the same.

Also, unlike in English papers, *I do not allow direct quotes!* There are only two exceptions to this: definitions and statements of proven results, such as theorems, may be copied from original sources. In this case, make sure you cite properly.

Important writing instructions.

1. DO NOT write anything you don't understand!!! Either (a) understand it or (b) delete it.

2. Don't quote anything. In fact, don't use quotation marks at all. The exception is statements of theorems and sometimes definitions.

3. In the introduction, provide motivation. This is mathematics, so that means a problem we wish to solve. This is theoretical mathematics, so the problem can be a pure math problem, not necessarily one a person on the street would care about. Then give an outline of the paper, which is essentially an informal explanation of how you'll solve the problem.

4. Unless you can think of something really good, just omit the conclusion. Generally, conclusions are pointless.

5. Prove *at least* one major result. You can and should assume anything we've covered in the course, and in any prerequisite course. Give references for anything else you don't prove.

6. Use LaTeX properly, expecially bibliographies and cross-references.

Topics. Many of the topics below are broad, so I recommend narrowing down your focus. You can also come up with your own topic, as long as I approve it ahead of time.

1. Computational complexity. The idea of complexity theory is to give a rough estimate of the number of basic computer operations necessary to carry out an algorithm. We will study several algorithms in this course whose efficiency (or lack of it) is important in many applications, including cryptography. *Maxwell*

2. Fast multiplication. The basic arithmetic operations are, not surprisingly, fundamental for any kind of software. Any even tiny increase in efficiency in these operations adds up very quickly. This project concerns itself with specific techniques used to do arithmetic quickly. *Heidi, Esequiel*

3. Quadratic reciprocity. We will be covering quadratic reciprocity, but only proving some special cases. There are over a hundred known proofs of the general case—present one. *Paeshence*

4. Quadratic forms. There are numerous projects that can be done on quadratic forms: solutions to $x^2 + dy^2 = n$ and the class number problem, Minkowski's method using the "geometry of numbers", solutions to $x^2 + y^2 + z^2 + w^2 = n$, and so forth. *James, Emily*

5. Pell's equation. Pell's equation, $x^2 - dy^2 = 1$, can be solved explicitly using continued fractions. *Yoko*

6. Rational approximation. Given an irrational number α, it is useful to know rational numbers which are "close" to α. This can be done with continued fractions, though there is a limit to how good any such approximation can be. *Brianna*

7. Error-correction codes. Suppose you wish to determine a chosen number between 1 and 16 with the minimum number of yes or no questions possible, but the chooser is allowed to lie in answer to one of your questions. What do you do? Practically speaking, when transmitting a digital message, there are bound to be errors in the transmission. Error-correction codes are methods used to fix errors with the minimum amount of redundancy. Some forms of cryptography, such as the McEliece cryptosystem, are based on error-correcting codes. *Nick*

8. Lattices. Intuitively, a lattice describes the structure of a crystal in n-dimensional space. Given a fixed lattice point (say, the center of one atom), what is the distance to the next nearest lattice point? This is an extremely difficult problem, with applications to data storage and fruit arrangement. *Leticia*

9. Encryption schemes. There are a number of different cryptography systems and techniques that are used in practice. Some of these include knapsack encryption, Diffie-Hellman, and elliptic curve cryptography. *Chris*

10. Arithmetic functions and Moebius inversion. Many properties about integers can be expressed and discovered by using a class of functions called "arithmetic functions". One famous example is the Euler totient function. There are various techniques used to derive properties of these functions, the most important of which is Moebius inversion. *Ryan*

11. Diophantine sets and Hilbert's 10th problem. Given a system of polynomial equations, one can ask whether there are any integer solutions. Is there some method for determining the answer to this question? This is Hilbert's 10th problem, and its answer is now known to be "no"! *Abraham*

12. Elliptic curves. Both the proof of Fermat's Last Theorem and various cryptosystems make use of elliptic curves. Elliptic curves are important because they have many interesting properties. This project should describe some of the more basic properties, possibly including a statement of the Mordell-Weil Theorem. *Oribay*

13. Unique Factorization. A basic result in number theory is the existence and uniqueness of factorization of positive integers into primes. The essence of the proof of this result is made clearer by studying certain "algebraic integer" systems where unique factorization fails. Moreover, algebraic integers are important in their own right, since their study in this context leads to the first modern insight into Fermat's Last Theorem and to results concerning the decomposition of integers into sums of squares. *Ben*

14. Fermat's Last Theorem and Other Diophantine Equations. The most famous theorem in number theory, possibly in all of mathematics was stated by Fermat in the margin of an ancient text by Diophantus that he was reading. "Unfortunately," he wrote, "the margin is too small to contain the proof." A proof of Fermat's Last Theorem was given by Andrew Wiles in 1994. *Nathaniel*

15. Mersenne primes and the Lucas-Lehmer test. The record-holder for the largest known prime has always been a Mersenne prime. Generally speaking, it is difficult to test a very large number (say with thousands of digits) for primality. But those of the form $2^p - 1$ can be tested by a method due to Lucas and Lehmer. *Abeneezer*

16. Primality testing. In 2002, Agrawal, Kayal, and Saxena made the biggest breakthrough to date in primality testing: a polynomial-time algorithm which determines if a given number is a prime. Most startling, their paper is only 9 pages long, and can be understood by anyone who has finished this course. *Jack, Othilie*

17. Factoring. The security of RSA is based on the presumed difficulty of factoring. There are numerous algorithms for factoring more quickly than with brute force—present one of these. *Keavin, Ashwin*

18. p-adic numbers. Given a prime p, the p-adic numbers are a number system with many strange but useful properties, such as that the sequence $p, p^2, p^3, p^4, \ldots$ converges to 0. *Emmanuel*

19. Hensel's Lemma. For a prime p, it is not hard to check if a polynomial has a root in $\mathbb{Z}/p\mathbb{Z}$—just test every element! Hensel's Lemma allows us to extend this answer to $\mathbb{Z}/p^e\mathbb{Z}$ quite easily. Together with the Chinese Remainder Theorem, this gives us a method for solving polynomials mod any n. *Marie*

20. Discrete Logarithm problem. The discrete logarithm is the inverse of modular exponentiation. The difficulty of calculating it is at the heart of many cryptographic protocols. *Marvin*

21. Cyclotomic polynomials. The study of the roots of unity is central to much of number theory. To study roots of unity, we instead consider the theory of cyclotomic polynomials—the polynomials whose roots are exactly the roots of unity. *Alicia*

22. Finite fields. The finite fields are the natural generalizations of $\mathbb{Z}/p\mathbb{Z}$ when p is prime. They have many nice properties, and are central to much modern number theory and computer science. *Billy*

23. ____________________________. Pick your own topic! Be very careful—an unwise choice can easily derail a paper. Ask me well in advance of the regular topic-choice deadline in case there are major problems with your idea.