Final Project Ideas, Guidelines, and Rubric

This project is open-ended, and I want you to do something that interests you. You might want to cover a section of the book that we didn't cover in class, or maybe number theory is related to something that you're studying in another class. If you have an idea, just let me know.

There are some project ideas in this document, provided by previous instructors of this class. (Some topics may not make sense because we haven't covered them yet.) You can look through the list to see if anything is interesting to you. You can also flip through our textbook to find interesting topics.

Timeline

(The first two dates are deadlines. It's probably better if you choose a project sooner rather than later.)

- Mon. 11/7. Let me know a few topics you are interested in by. (They don't have to be very specific.) I can respond with some project suggestions.
- Mon. 11/14. Let me know your project choice.
- Tues. 11/29. In-class presentations.
- Mon. 12/5. Final paper due

Components

Paper

Historical/Background Information (around 1/2-page to a page, single spaced) Give the background on the problem that you are studying. Who has studied this problem? Which mathematicians have contributed to the solution? Why is this problem interesting/important? What connections are there to history, politics, culture? How are the mathematical conventions of other cultures/times relevant?
The prompts vary in the type of background information that is most appropriate. I don't expect your paper to give an exhaustive account of all historical connections. I want you to tell me a compelling story. Give me a reason to care about the problem, or demonstrate that some prominent historical figures were interested in the math.

Examples Motivate the math by working out in detail simple and illuminating examples. (For example, in the divisibility project you should demonstrate rules of divisibility on explicit numbers.) Try to find examples that demonstrate key aspects of the proof that you will write down abstractly. The abstraction will make more sense if you ground it in concrete numbers.

Proof In each of the projects you should prove (at least some of) the relevant mathematical facts. You should give a complete, clear, and understandable proof. You don't need to come up with the proof on your own; you should be able to find references that explain the math. Make sure you understand the math and rewrite it in "your own words" when possible. (Sometimes an equation is just an equation, and you can't exactly "put it in your own words." But you should understand the math that you write).
For some projects it's more obvious what to prove than others. For example, in the Lagrange's four squares theorem project, you should prove the four squares theorem. For others, it is less clear. I can help you find something to proof.

Citations The paper should be well cited. You may use MLA or APA format. Wikipedia is a good starting place for understanding the math/finding other references, but you should have reputable sources in your final paper.

Presentation

Time The presentation should be under 10 minutes.

Topics You may include in your presentation any compelling/relevant material. You probably will not have time to give a complete proof of anything. You'll need to decide what to include and what to leave out. The presentations should be understandable. Don't blow through high-level math and leave your audience in the dust. Ask questions if you can. Engage your audience! Choose exciting material to present!

Media Sometimes the best way to convey your point is by keeping things simple. Depending on your presentation, you might want to give a talk using the chalkboard exclusively. You may also combine the use of the board with other media, if that works for your presentation. The room has HDMI and VGA hookups, if you would like to use the projector. You are welcome to make a slide show, but keep the number of equations per slide low.

Rubric

Paper			
	Background		
		Factual Content: Addresses important/relevant facts	5
		Motivating Content: Piques interest, motivates study	5
	Example(s)		
		Choice of Example: Simple and illuminating	5
		Clear Presentation: Easy to follow, good typesetting	5
		Accuracy of Mathematics	6
		General Understanding	6
	Proof		
		Sophistication of Mathematics: Includes appropriately challenging math	10
		Clear Presentation: Easy to follow, good typesetting	5
		Accuracy of Mathematics	6
		General Understanding	7
	General		
		Citations	10
		Writing Quality: Good grammar/spelling/flow/logic	5
Presentation			
		Time: Under 10 minutes	5
		Content: Includes engaging material	10
		Style: Well prepared, good use of board/other media	10

Some Topic Ideas

Thank you to Tori Akin and Asilata Bapat for allowing me to adapt some of their ideas.

1. **Formulas for primes** We know that there are infinitely many primes, but how do we find them? Some computers are devoted entirely to the search for large prime numbers. Are there any tricks to finding primes? Of course! For example, we can use the formula $(n)(n+1)+17$ to generate some primes. Does this formula always work? When and why might it fail? What other formulas do we have for generating primes? Do they ever fail and produce a composite number instead of a prime number? What are the largest known prime numbers and how have we found them?

   You could think about algorithms for computationally testing whether or not a number is prime. It's very slow to check by division. But there are fast ways using modular arithmetic. A famous method of testing for primes is the Sieve of Eratosthenes. What other methods exist? Which are the fastest? Do they always work?

   For a different sort of challenge you could code your own prime test!

2. **Mathematical Induction**
   Here's a cool pattern.

$$\begin{aligned} 1 &= 1^2 \\ 1+3 &= 2^2 \\ 1+3+5 &= 3^2 \\ 1+3+5+7 &= 4^2 \\ 1+3+5+7+9 &= 5^2 \\ &\vdots \\ 1+3+\cdots+(2n-1) &= n^2 \end{aligned}$$

   We can test lots of numbers to see that this pattern seems to hold. But examples aren't the same as proving that something is always true. How can we make sure that this is still true when we add up very many odd numbers? The trick is mathematical induction!

   What is mathematical induction? What are some examples of how we use induction to prove that a pattern holds for all natural numbers? What is well-ordering and how is it related to induction? Try number 2.20, and 2.21 in the book!

3. **Secret Sharing** Suppose you are the president of a country with nuclear weapons. You want to choose some very responsible people to have to the launch code for these weapons. Would you trust the code with anyone? What if you could split the code up between 3 different people so that no one individual has the code but any 2 of them together could recover the launch code?

   We can use polynomial interpolation to divide information between as many people as we want. What is polynomial interpolation? How does the algorithm change if we want any 5 people to be able to recover the secret? How large is the polynomial?

   Related, and for an extra challenge, we know that 2 points determine a line, but how many points does it take to determine a parabola? a cubic function? What does it mean to "determine"? What is a basis?

4. **One Time Pad** A very secure way to encrypt data is using a method called one time pad. It is quite difficult for an outside observer to attack, but one time pad is computationally expensive (what does that mean?) What exactly is one time pad? In this project you'll think about mod 2 arithmetic and random number generation!

   What methods do we have to randomly generate numbers? What are the pros and cons of this encryption method?

5. **Vigènere Cipher** You know how shift ciphers work. But what if instead of a standard shift we did several different shifts at once? We could add 13 to the first letter, 1 to the second, 20 to the third, and then repeat this sequence of shifts. Now, a frequency analysis alone won't help us decrypt the message. We need new techniques. What is Kasiki elimination? What is the Friedman test? Historically, how did mathematicians challenge each other with this sort of puzzle?
   This project is (somewhat) related to the Euler-φ function. What is the Euler-φ function and how is it related? Possibly you could prove Euler's product formula. What key lengths are good choices? Which are bad choice?

6. **Fermat and Beyond!** In 1637 Fermat wrote a note in the margins of a copy of *Arithmetica* about a fact of mathematics that wasn't proved until 1994! What was the fact? No three positive integers a, b, c can satisfy the equation $a^n + b^n = c^n$ for any n greater than 2.

   Notice, when $n = 2$, the set $\{a, b, c\}$ is a Pythagorean triple. We know that many of those exist. How many? Infinitely many? What does it mean to be a "primitive" triple? How can we generate "primitive" triples?

   Is Fermat's last theorem still true when we work in modular arithmetic systems? Let p be prime and consider examples mod p. Here's an amazing fact of modular arithmetic: $(a + b + c)^p \equiv a^p + b^p + c^p$ mod p. Why is that true? Does that give us a way to find mod p solutions to the equation?

7. **Divisibility** In class, we've seen that to check if a number is divisible by 3, we just have to sum the digits and check if that sum is divisible by 3. We've covered similar rules for 5 and 9. How do we check if a number is divisible by 7? Can you use modular arithmetic to prove it? What about 11? 99? or 101?

   Now, let's work in a different base. Let's write our numbers in base 60 (like the ancient Babylonians, I think). Is there a quick way to check whether or not a number is divisible by 2, 3, 5? by 59?

8. **Fibonacci Numbers** You could do many different projects with the Fibonacci numbers, but here is one direction. Look at the greatest common divisor of any two Fibonacci numbers. You'll notice that it is also a Fibonacci number. What's more, let f_n be the nth Fibonacci number. Then $\gcd(f_n, f_m) = f_{\gcd(n,m)}$ Amazing! (This proof requires induction).

   For a start, what if we look at two adjacent Fibonacci numbers? Can we use the Euclidean algorithm to see that $(f_n, f_{n+1}) = 1$?

   Can you show that $f_{m+n} = f_{m+1}f_n + f_m f_{n-1}$?

   If $m|n$ can we see that $f_m|f_n$?

9. **Polynomials** We know $\mathbb{Z}$ satisfies axioms A1–A4, M1–M3, D. Now, what if instead of integers, we think about polynomial functions? How can we determine the gcd of two polynomials? How does

polynomial long division work? Are polynomials a special set? A ring, perhaps? What are the additive inverses? Are there multiplicative inverses? What does it mean for a polynomial to be "prime?" Can we do modular arithmetic with polynomials?

10. **Imaginary numbers and Gaussian integers** We know $\mathbb{Z}$ satisfies axioms A1–A4, M1–M3, D. But what happens if we add an imaginary number to the mix? How does that work? If we take $\mathbb{Z} \bigcup \{i\}$ (where $i^2 = -1$) is that set closed under addition and multiplication? I think not! Instead, we need $\mathbb{Z}[i]$. What does that mean? Well, we need to include everything of the form $a + bi$ for $a, b \in \mathbb{Z}$. How do multiplication and addition work in this set? What properties hold? Do we have inverses? identities? Are there "prime" elements? Does the Euclidean algorithm work?

    Try starting with 1.25 in the book

11. **Lagrange's Four Square's Theorem**

    I know that I can write some numbers as the sum of two squares. For example

$$\begin{aligned} 4 &= 0^2 + 2^2 \\ 5 &= 1^2 + 2^2 \end{aligned}$$

    However, some numbers just can't be written as the sum of two squares. We just can't do it for 6, 7 or 12 for example.

    But amazingly, every positive integer can be written as the sum of four squares. What!? Do some examples to see for yourself.

    So, how can we prove this? Using modular arithmetic!

12. **Pascal's triangle**

$$\begin{array}{c} 1 \\ 1\ 1 \\ 1\ 2\ 1 \\ 1\ 3\ 3\ 1 \\ 1\ 4\ 6\ 4\ 1 \\ \vdots \end{array}$$

    You know what happens when you expand $(x + y)^2$. But what are the coefficients when you expand $(x+y)^3$? $(x+y)^4$? $(x+y)^{10}$? Is there a pattern? Do the coefficients appear in Pascal's triangle? (You can show this by induction, or you can give a combinatorial argument).

    If you have 10 different bracelets, how many ways can you choose exactly two of them to wear? Why are these problems related to each other and Pascal's triangle?

    Now, take things one step further. Let's do the arithmetic mod p for some prime. What do we get for $(a + b)^p \mod p$?

13. **The Game of Nim** In this game two players have three piles of coins. Players take turns removing coins from one pile at a time. The goal is to take the very last coin. Is there a winning strategy? You'll use mod 2 arithmetic. You'll also learn about the "nim-sum" which is an operation satisfying some familiar properties. Which properties does it satisfy?

    For a further challenge, you could look at "nim-like" games and the generalization of the nim-sum.

14. **Dance and Mathematics** Check out this New York Times dance review: `http://www.nytimes.com/2013/12/06/arts/dance/moses-es-comes-to-brooklyn-academy-of-music.html?smid=pl-share` And see this companion video: `https://vimeo.com/74732379`

    The movements in the piece are partially based on fractal geometry. What is a fractal? What is self-symmetry? What other fractals do you know?

    You could look into the Cantor set as an example of a fractal. How big is the Cantor set? As big as the set of real numbers?

    You could look at Pascal's triangle mod 2. This behaves like a fractal. Why? What is Luca's theorem? You'll learn some combinatorics to understand binomial coefficients.

15. **Constructible Numbers** Did you hear the rumor that the Alabama legislature was changing the value of π to 3? While that's not true, something surprisingly similar happened in 1897. What is the Indiana π bill? What did it concern? What is squaring the circle? What are constructible numbers? Give several examples. Perhaps you could prove that $\sqrt{n}$ is constructible for any $n \in \mathbb{N}$.

16. **Pitch Class and Tuning** You can vibrate a string of a certain length to get a particular note. You can cut that string in half to get the same note one octave higher. How do you have to cut the string to get a perfect fifth? What is a perfect fifth? What is pitch class? What does it have to do with mod 12 arithmetic? How is our current scaling different from that of Pythagoras, and why?

17. **Math and magic tricks** Do you know any magic tricks that are just mathematics in disguise? Find an interesting trick of this kind. What is the trick? Can you justify why it works?

18. **Other possible topics** Magic squares, Euler-φ function, Catalan numbers, something from any part of the textbook, anything that interests you!