Math 303, Fall 2022
David Singer
Course Information

Text *A Friendly Introduction to Number Theory, fourth edition*, by Joseph H. Silverman, Pearson, 2013 (ISBN 13 978-0-321-81619-1).

Other Materials A calculator or computer will be useful in doing some computations. If you are familiar at all with Mathematica, it is powerful enough to do all computations. You will also be able to do calculations using the SAGE calculator (thanks to some enterprising CWRU students), which is now in its fourth edition.

Prerequisites The official prerequisite is MATH 122. Most of the work really only requires some comfort with high school algebra, although the discussion of elliptic curves will use calculus a bit.

Office Hours I will have in-person office hours on Monday and Wednesday, and Zoom office hours at other times. I enjoy talking to students, so do not hesitate to see me, either by schedule, appointment, or lucky drop-in.

Homework There will be homework problems assigned on a regular basis, which you may submit in person or via Canvas. Handwritten solutions must be written clearly and neatly. For electronic submissions, I prefer that the format you use is PDF. Word files sometimes do not display properly because of font issues, and it is easy to save a word document as a PDF. You may also upload scanned documents, but make sure they are legible; dark ink on white paper is optimal in that case.

Important: I grade all homework myself and will write comments to give you personalized feedback. If you submit electronically, Canvas allows me to attach comments to your paper, and I will use that feature. Please leave some **blank spaces** on each homework page, so that I can insert the comments on your paper.

Grading is a lot of work for me, but I am very happy to do it if it will help your experience in the class! But please make an effort to make your paper **readable**. **Highlight your answers** to speed up the grading process. But show your work, so I can see how you got the answers. I will post solutions.

On the top of the front page of each assignment, please put your name in the upper left corner, followed by the assignment number and date.

Grading Policies Homework assignments will count for 30% of the grade. Problems are due roughly once a week (see schedule below). Each problem or problem part is worth one point, with half points assigned at my discretion. The real purpose

of the homework is to help you learn the material, so turning in assignments (even incorrect ones) also counts toward the homework grade, and I often allow resubmission when an assignment has had serious errors.

Since I consider the homework to be a vital part of learning, I generally accept homework turned in late, particularly if it is only one class period. However, repeatedly doing so will count against your grade. Let me know if you are having difficulties or have fallen seriously behind; I will be glad to work with you to help you catch up.

Each group of up to three students will prepare a project on a topic of their choice relating to the subject matter of the course, which will count for 20% of the grade. The topic should be selected by no later than **Monday, October 3, 2022**. (The first to choose a topic gets it; emailing your request provides you with a time stamp.) A rough draft/progress report on the project will be due on **October 21, 2022**. The **absolute deadline** for submission of completed project is **December 9**. Please consult Information on References for the proper choice and citation of references. There will be a midterm exam scheduled for **Wednesday, October 19, 2022**, which will count for 20%. The final exam will be on **December 14, 8:00–11:00AM** and will count for the remaining 30%.

Projects There are many interesting topics in number theory that are not in the syllabus. A list of suggestions is attached to get you started. Each group of up to three students will select a topic (from a list provided or elsewhere) and prepare a report on the topic. The report may either take the form of a paper or a powerpoint or similar presentation. Written reports should be about five pages per student (2000 words), not counting tables and graphics. Every project should have at least two (preferably three) reputable, published sources, and specific citations should be given. Any material taken from sources should be cited with specific page numbers. If you are preparing slides, you may include citations as notes attached to the slides or in the slides themselves. You do not need to submit a full written report if you prepare slides, but you should submit a supplement with any important details that are not in the presentation.

Midterm The midterm exam will cover material from the first 11 chapters plus a little bit from chapters 16-18 and 28. The usual rules of academic integrity apply: you may consult books or notes but not other people, in person or online.

Schedule Below you will find a schedule of topics covering the first two-thirds of the semester. Also included are the dates of homework assignments. The schedule is subject to change!

Continued on the next page.

	Schedule of Readings and HW		
Date	Topic	No.	Due
8/29	1. What is Number Theory	1	9/2
8/31	2. Pythagorean Triples		
9/2	3. Pythagorean Triples	2	9/7
9/7	5. Divisibility and GCD		
9/9	6. Linear Equations and GCD	3	9/12
9/12	7. Factorization and Fundamental Theorem		
9/14	Proof of Fundamental Theorem		
9/16	8. Congruences	4	9/19
9/19	9. Congruences, Powers, and FLT		
9/21	(28). Primitive Roots		
9/23	10. Euler's Formula	5	9/26
9/28	11. Euler's Phi Function		
9/30	11. Chinese Remainder Theorem	6	10/3
10/3	11. Euler's Phi Function	7	10/7
10/7	16. Powers Mod m	8	10/10
10/10	17. kth roots Mod m		
10/12	18. Introduction to RSA Cryptography		
10/14	18. RSA continued	9	10/17
10/17	Review		
10/19	Midterm Exam	*	
10/21	20. Squares Mod p		
10/26	21. -1 and 2 Mod p		
10/28	22. Quadratic Reciprocity	10	10/31
11/2	22. Jacobi Symbol		
11/4	29. Primitive Roots and Indices	11	11/4
11/7	41. Cubic Curves and Elliptic Curves		
11/9	Elliptic Curves	12	11/11
11/11	43. Elliptic Curves Modulo p	13	11/14
11/14	Elliptic Curve Cryptography	14	11/18
11/16	TBA		
11/18			
11/21			
11/235			
11/28			
11/30			

Here are some possible topics to consider for projects; many of these topics have been done by students in previous years. Please report outdated links. You need prior approval to choose a topic not on this list!

(1) Areas of Pythagorean Triangles

It is easy to see that 6 is the smallest integer which is the area of a right triangle with integer sides. An integer is called "congruent" (unfortunately!) if it is the area of a triangle with *rational* sides. What is known about such numbers?

(2) Bertrand's postulate

Is there always a prime between n^2 and $(n+1)^2$? Chebychev solved Bertrand's conjecture, that for any $x > 3$ there is a prime number between x and $2x - 2$. Erdos simplified the proof. What is known about this kind of distribution of primes?

(3) Carmichael Numbers

A Carmichael number is a number n which is not a prime for which $a^{n-1} \equiv 1 \pmod{n}$ for all a with $1 \leq a \leq n-1$. What is known about Carmichael numbers? How many are there? How can they be constructed?

(4) Catalan's Conjecture

$2^5 + 7^2 = 3^4$ and $1414^3 + 2213459^2 = 65^7$ are two solutions of the Fermat-Catalan equation. It is conjectured that there are only finitely many solutions. This generalizes Catalan's conjecture that 2^3 and 3^2 are the only consecutive powers. (Catalan's conjecture was only recently solved, by Mihailescu.)

(5) Continued Fractions

The Euclidean algorithm gives a recipe for generating continued fractions. What are they, and what are they good for - especially in factoring integers? A good article to read is Guerzhoy

(6) Egyptian fractions

This offbeat topic is about writing fractions as sums of different fractions with 1 in the numerator. For instance, 1/3 + 1/11 + 1/231 = 3/7. There is a "greedy algorithm" and also an "odd greedy algorithm" for finding these sums.

(7) Fermat Primes and constructible polygons (This is challenging)

A Fermat number is a number of the form $n = 2^{2^k} + 1$. When $0 \leq k \leq 4$ these numbers are known to be primes. Gauss used such numbers to construct regular polygons with compass and straightedge. What is the relationship between Fermat numbers and constructible polygons?

(8) Fermat Primes II

An interesting problem is to test whether a Fermat number is a prime. A test was derived by Pépin. How does this test work? Are there other methods out there?

(9) Fibonacci Numbers and Prime Numbers

When are Fibonacci numbers prime, and when are Fibonacci numbers divisible by a prime p? More generally, how do Fibonacci numbers behave mod p?

(10) Fibonacci Squares

The number 144 is the only Fibonacci number that is a perfect square. see J. H. E. Cohn, "Square Fibonacci Numbers, Etc." Fibonacci Quarterly 2 1964, pp. 109-113.

(11) Generalized Fermat Numbers

A number of the form $a^{2^n} + 1$ is called a Generalized Fermat Number. For example, $1372930^{131072} + 1$ is known to be a prime number (with over 800000 digits). What is known about these numbers? What prime numbers are known to be factors of such numbers? See, e.g., Factors of Generalized Fermat Numbers, by ANDERS BJORN AND HANS RIESEL, Mathematics of Computation, Vol. 67, No. 221 (Jan., 1998), pp. 441-446.

Bjorn and Riesel

(12) Goldbach conjecture

Can every even integer be written as the sum of two primes? See

Richstein

for a discussion complete with large list of references.

(13) Highly Composite Numbers

These are numbers which have more factors than any smaller number; the sequence begins 1,2,4,6,12,24,36,48,60,120,180. An article by Alaoglu and Erdos in Transactions of the American Mathematical Society, 56 (1944), can be found at `http://www.jstor.org/stable/i308266`. See Wikipedia article for starting explanation and link to an algorithm by Kedlaya.

(14) Infinitely many primes (this is a very challenging topic)

Euclid gave the familiar original proof that there are infinitely many primes. Euler gave a deeper proof using the Riemann Zeta function $\zeta(s) = \Sigma\frac{1}{n^s}$. What is the idea behind this proof? How does it shed light on the number of primes less than a given value?

(15) The Jacobi-Madden Equation

Euler proposed the problem of finding integers satisfying $A^4+B^4+C^4+D^4 = E^4$ in 1772. Noam Elkies (1988) found an infinite sequence of solutions with

$D = 0$ and the other terms non-zero, disproving a conjecture of Euler that such solutions did not exist. In 2008, Lee Jacobi and Daniel Madden found and infinite set of non-zero solutions with $E = A + B + C + D$. See American Mathematical Monthly 115 (3)March, 2008, 220–236, for how they did it.

(16) Mersenne Primes

A Mersenne prime is a prime number of the form $n = 2^p - 1$, where p is a prime. There is a test called the Lucas-Lehmer test for determining whether $2^p - 1$ is a prime. As of December 2018, there are 51 such prime numbers currently known. Explain the Lucas-Lehmer test.

(17) Pell's equation

This is one of the most famous problems in number theory, going back to Archimedes. A simple example is $x^2 - 2y^2 = 1$ (x and y have to be integers, of course.)

(18) Polygonal Numbers

A polygonal number is a number that can be represented by pebbles arranged as a regular polygon. Gauss proved that every number is a sum of three triangular numbers. (See also the four squares theorem.) Cauchy proved that every number can be written as a sum of n polygonal numbers of order n for all $n \geq 3$. Explore the features of these numbers.

(19) Prime Number Races

Are there more primes of the form $4x + 3$ than of the form $4x + 1$? Well, there are infinitely many of each, but if we cut off at some maximum valume, there seems to be a bias. What is the story? See Granville Greg for some information on this. (Granville, Andrew, and Martin Greg. "Prime Number Races." The American Mathematical Monthly 113.1 (2006): 1-33.)

(20) Prime Recurrences

A prime p is a Sophie Germain prime if $2p+1$ is also a prime. The sequence $2, 5, 11, 23, 47, \ldots$ does not continue to give new primes. Are there long sequences of this type? If the next term is defined to be the largest prime divisor of $2p_n + 1$, does the sequence diverge or cycle? This question can be asked for other formulas, such as $3p + 1$ and $p^2 + 1$.

(21) Primes in Arithmetic Progression

The sequence

$$\{121174811, 121174841, 121174871, 121174901, 121174931, 121174961\}$$

is made up of primes in arithmetic progression. How about longer such sequences? See the paper by Green and Tao at `http://arxiv.org/abs/math.NT/0404188`

(22) Primitive roots

The decimal expansion of 1/7 repeats after 6 digits. The expansion of 1/19 takes 18 digits to repeat. This can be reformulated by saying that 10 is a primitive root mod 7 and also mod 19. What is known about the general question? (See `https://arxiv.org/pdf/math/0412262v2.pdf` for some current information.)

(23) Smooth Numbers

Highly composite numbers (see above) are examples of smooth numbers, numbers with small prime divisors. These are quite important for certain applications in computational number theory. A paper by Andrew Granville can be found at Granville

(24) Stephen Colbert Numbers

It is known that $78557(2^n)+1$ is *never* a prime number. (So 78557 is called a Sierpinski number). Is 78557 the smallest number k for which $k2^n+1$ is never prime? There are only 17 candidates for smaller Sierpinski numbers. The "Seventeen or Bust" project aims to solve this problem by finding Stephen Colbert primes (yes, THAT Stephen Colbert). Find out more at `http://www.prothsearch.com/sierp.html`.

(25) The Sum of Four Squares

Leonhard Euler tried unsuccessfully for 25 years to prove that every positive integer can be written as the sum of four squares. The problem was solved by Lagrange. How was it done? What is known about writing numbers as a sum of four squares?

(26) The Sum of Two Squares (it helps to know about complex numbers for this one!)

Gauss proved that a prime number can be written as a sum of two squares if it is not congruent to 3 mod 4. Explain some of the ideas.

(27) Sums of cubes It is known that numbers of the form $9k+4$ and $9k+5$ can not be written as sums $x^3+y^3+z^3$ with x, y, and z integers (positive, negative or zero.) Can all other integers be represented this way? See "Cracking the Problem With 33" at `https://people.maths.bris.ac.uk/~maarb/papers/cubesv1.pdf`.

(28) Transcendental Numbers I (you need to be comfortable with infinite series)

A real number is called "algebraic" if it is the root of some polynomial with integer coefficients, and "transcendental" if it is not algebraic. Liouville gave a criterion for a number to be algebraic. He was then able to prove that $\Sigma_{k=1}^{\infty} 10^{-k!}$ is transcendental. How?

(29) Transcendental Numbers II (this is an advanced topic!)

It is known that e and π are transcendental. What other numbers are known to be transcendental, and how? (See, for example, the Gelfond-Schneider theorem).

(30) The Twin Prime Conjecture

This is the problem of finding infinitely many pairs of prime numbers differing by 2. In May 2013, Yitang Zhang announced a proof of the "bounded gap" theorem. See Zhang. There is an explanatory YouTube video at

`http://www.youtube.com/watch?v=D4_sNKoO-RA&feature=youtu.be`

Also, see the Blog at Kowalski

(31) Unique Factorization (This is a challenging topic)

Unique factorization of integers into primes can be extended to other rings of numbers. However, there are only finitely many integers q for which the ring of numbers of the form $a + b\sqrt{q}]$ have a Euclidean algorithm. (See H. Chatland and H. Davenport, "Euclid's Algorithm in Real Quadratic Fields", Canadian Math. Journal 2 [1950], 289-296.)