Mathematics 321: Number Theory

Fall 2018

Instructor: John Rhodes

Office: 208B Chapman, 474-5445

E-mail: `j.rhodes@alaska.edu`

Office Hours: M 1:00–2:00; R 11:30–12:30, or by appointment

Web page: `https://jarhodesuaf.github.io/M321.html`

Prerequisites: Math 265, or permission of the instructor

Credit Hours: 3.0

Textbook: Elementary Number Theory and Its Applications, by Kenneth Rosen, 6th edition, Addison Wesley

Class Meetings: TR 9:45 – 11:15, in Duckering 344

Exams: Midterm: 9:45-11:15, Oct. 16
Final: 8:00-10:00, Dec. 11

Course Overview and Goals:

Number Theory is, at least approximately, the study of the whole numbers, or integers. These are the numbers humans seem to develop an almost intuitive concept of, with little need for a formal development for anyone to feel they are valid and useful concepts. In the words attributed to the great number theorist Leopold Kronecker, "God made the integers; all else is the work of man."

The topics within number theory are varied, with some dating back to the ancient Greeks, and many on the forefront of current mathematical research. Many problems (but not all) can be stated fairly simply, though making progress towards solving them may require highly-developed tools drawn from other areas of mathematics. Examples include:

1. How are the prime numbers distributed? When listed in order, they appear rather to have rather random gaps between them, but in fact they pop-up with a rather precise regularity. A formal statement of this regularity is the *Prime Number Theorem*, first proved in 1896, by Hadamard and de la Vallée-Poussin independently, using Complex Analysis. It is believed that there are infinitely many pairs of primes that are 2 apart, but this *Twin Prime Conjecture* is an unsolved problem.

2. Given a polynomial equation, how many solutions does it have in the integers, and is there a way to find them all? For example $x^2+y^2=z^2$ has solutions $(3,4,5)$, $(5,12,13)$, and infintely many other such Pythagorean triples, all of which can be explicitly listed. However, for $n\geq 3$ the equation $x^n+y^n=z^n$ has no solutions in integers (except for the trivial ones with one of x or y zero). This was conjectured in 1637 by Fermat, and finally proved by Wiles in 1995, using extremely elaborate algebraic techniques building on decades of work of other recent mathematicians.

3. Every positive integer can be written as the sum of 4 squares, as Lagrange proved in 1770. Waring's problem asks to determine how many terms are needed to write every integer as a sum of kth powers. Waring posed the question in the 1700s and Hilbert proved in 1906 that for every k there was such a number of terms that sufficed for all integers, but its value is not in general known.

In this course, we'll focus on *elementary* number theory, which is that part of the field which does not draw heavily on other branches of mathematics. It served as motivation for the later development of the abstract algebra, so if you have taken an algebra course you will see some familiar material again, but with a different focus. While Number Theory was, and still is, studied for its own inherent interest, it has also become an important area of applied mathematics, as it underlies most computer security schemes. The course will introduce some of these applications.

Course Mechanics:

Class meetings will be run as interactive lectures. While I will be presenting material at the board, and you will be taking notes, I will also be asking for suggestions, ideas, and questions about the material as we go along. I don't expect 'correct' answers to these, but I do expect you to be actively following and participating — that makes the class more interesting for us all. I welcome questions as we go along.

Class attendance is expected, although I will not formally take roll. If you miss a class, you should get notes from another student. Homework assignments will be posted on the course web page, and you should make it a habit to check for new problems after each class.

Homework will be assigned daily, and generally due at class the following Tuesday. Assignments will be posted on the class webpage shortly after meetings. At the beginning of class, there may be a little time for simple questions on homework, but you should expect to get your homework questions answered during office hours.

You will also have some computer-based investigations to perform, using web-based resources or the software package Pari/GP. Pari is free, and easily installs on Windows, Mac, and Linux machines. A link to a web-page associated with the text, which contains a link to the Pari download site, is on the class webpage.

Grading of homework, whether proofs or calculations, will take into account not only correctness but also clarity of exposition. Expect to spend time and effort in presenting your work well.

I encourage you to work with others on the homework, and to share ideas for solutions, but you must *write up solutions independently.* You will learn nothing from simply copying a solution. Even though you may find you can't do every problem, you must make a reasonable attempt on them all. The entire homework assignment will be checked to be sure you have attempted everything. Selected problems will be graded completely.

Homework will be accepted without penalty until 5pm on its due date, either at my office or in my mailbox in the math department office. Beyond this, I will not accept *any* late homework that has not been cleared ahead of time or is not due to a genuine emergency (e.g., a death in the family).

Examinations: The midterm exam will be 1.5 hours in length. You will need to state and understand definitions and theorems, be familiar with examples, and prove some relatively straight-forward statements.

The final examination will consist of two parts: an in-class part that will focus on definitions, examples, and 'routine' proofs, and a take-home part that will consist of more challenging proofs which you will be able to work on for at least several days. For the take-home part you will be able to refer to your textbook, class notes, and homework, but nothing else.

Any form of cheating on these exams will be dealt with harshly. At a minimum, the full examination (take-home and in-class) will receive a score of zero. Depending on my concern with the extent of cheating, any incident may result in a course grade of F, and I may also request a University hearing which could result in suspension or expulsion. Please note that evidence of collaboration on work in mathematics is usually obvious, so even if your personal honor is worth nothing to you, cheating is a foolish risk to take.

Missed examinations that are not approved in advance will result in a zero on that exam. No make-up exams will be given except in extreme circumstances (e.g., family death, documented illness, etc.). Notifying me by email or a note that you will miss an exam is not sufficient for advance approval; you must speak with me to be excused.

Auditing of this course will only be allowed for those who agree to attend regularly, submit homework, and take the midterm exam.

Course Grades will be assigned using the following weights:

Homework	30%
Midterm	30%
Final Exam	40%

Letter grade bands are: 90 – 100% A; 80 – 89% B; 70 – 79% C; 60 – 69 D; 0 – 59% F. Scores near the ends of the bands will receive a $\pm$. I may adjust bands (but only downward) if I feel that is necessary for fairness. A stellar grade on the final may also overcome earlier weaker work and improve a student's final grade beyond the straight weighting scheme.

Other Policies:

Course accommodations: If you need course adaptations or accommodations because of a disability, please inform your instructor during the first week of the semester, after consulting with the Office of Disability Services.

University and Department Policies: Your work in this course is governed by the UAF Student Code of Conduct. The Department of Mathematics and Statistics has specific policies on incompletes, late withdrawals, and early final exams at `http://www.dms.uaf.edu/dms/Policies.html`.

Tentative Schedule:

Week	Chapter
Aug 27	1
Sept 3	1, 2
Sept 10	3
Sept 17	3,4
Sept 24	4
Oct 1	5, 6
Oct 8	7
Oct 15	Midterm Exam, 8
Oct 22	8, 9
Oct 29	9
Nov 5	10
Nov 12	11
Nov 19	13
Nov 26	14
Dec 3	12 (if time permits)
Dec 11	Final Exam