Theory of Numbers

Math 319, Spring 2009

Basic Course Information

- Description: In this class we will study the structure of numbers. The integers, rational numbers, and related groups and rings of numbers permeate mathematics. Reknowned for its plethora of easy-to-state unsolved problems, cryptographers make use of what can and cannot (yet) be done to ensure security in computers, telephones, GPS, key-less entry, and other transmissions. We will use our experience from grade-school to explore the structure, use computers to perform experiments and develop conjectures, and write proofs based on axioms to lay out a logical framework.
- Course philosophy: This course will be taught using inquiry-based learning and will thus be heavily problem-based. You will *frequently* encounter terms that you do not know. Look them up, just as if you were reading a novel.
- Prerequisite: Math 319 (Introduction to Mathematical Proof)
- Required materials:
  - *Number Theory* by Andrews
  - *Higher Arithmetic* by Davenport
  - Well organized notebook or binder (you will often need to reference or re-submit problems)
- Programming languages: We will make use of one or more of the following programming languages:
  - *Maple* (on campus computers)
  - *Sage* (free online access & free to download)
  - *PARI / GP* (free PC download, free online access through SAGE)
- Textbook resources on reserve in Milne Library:
  - *An introduction to the theory of numbers* by Hardy and Wright.
  - *Solved and unsolved problems in number theory* by Shanks.

Contact Information

- Your instructor: Dr. Patrick Rault
- I have been studying number theory for 10 years and completed a Ph.D. in the subject six months ago. Though I am relatively new to SUNY Geneseo, I hope to inspire a love of the subject in you.
- The best way to reach me is by e-mail:
  - **rault@geneseo.edu**
- I hold two office hours a week and reserve a third for special appointments. Office hours are a place where **anyone** may ask questions. Use them regularly and your understanding will improve, no matter whether you are doing well or poorly in the class.
  - **Office**: 326C South Hall
  - **Office Hours**: Mondays 5:45-6:45pm (in 336 South Hall), Thursdays 2-3pm
  - **Monday problem session**: The Monday office hour (listed above) is a problem session specifically for Number Theory students. We will be in a larger classroom in hopes of higher turnout.
  - **Appointments**:
    - If you are not available during my regular office hours and need to schedule an appointment with me outside of class, please first check my schedule on my website. Then e-mail a *list*

of the appointment times you are available so I can schedule a one-time extra office hour (there may be other requests, and I will likely invite the whole class).
    - I expect that you've already asked or consulted someone about the problem. Working with other students challenges your own understanding and can solve minor misunderstandings.
  - **Off-topic office hour:**
    - Thursdays 3-3:30pm
    - This office hour is specifically for off-topic questions. For example, if you have a question about the Riemann Hypothesis, careers in mathematics, applications of linear algebra, or how a class problem relates to deeper mathematics, this is the time and place.
- All of this information (including a copy of the syllabus) will be available at both of the following:
  - **Course website: www.geneseo.edu/~rault/**
  - **Mycourses:** https://mycourses.geneseo.edu/

Class Structure

- **Problem sets:** I will assign frequent homework assignments in class in the form of problem sets. For these problem sets you may use any axioms and lemmas from your axiom and lemma lists (see below) and reference any problems from previous problem sets which you have proven.
  - Deadlines: Each problem set will have a deadline. However, any *Proof, Disproof, or Salvage if Possible* problem may be resubmitted or submitted late for partial credit (see below).
  - Problem types: There are several types of problems which appear on problem sets. The point values are as follows. I reserve the right to give extra points for an outstanding solution.
    - *Numerical*:
      - 4 points: an exhaustive answer to the problem
      - 3 points: an answer which shows that you understand the problem
      - 2 points: a major contribution to the problem which also has a major flaw
      - 1 point: a contribution to the problem
    - *Exploration*:
      - 4 points: a rare exhaustive answer to the problem
      - 3 points: an insightful answer to the problem
      - 2 points: a major contribution to the problem
      - 1 point: a contribution to the problem
    - *Proofs:*
      - 4 points: fully correct problem
        - NOTE: every step MUST be justified by reference to definitions, axioms, lemmas, previous problems, etc.
      - 3 points: late problem (includes corrected problem)
      - 2 points: proved something significant related to the problem (may be later upgraded)
      - 1 point: late problem that has become trivial due to a new problem
    - *Disproofs & Salvages:*
      - 4 points: disproof, good salvage, and proof of salvage
      - 3 points: disproof and proven salvage
      - 2 points: disproof and either a conjecture or a salvage attempt
      - 1 point: disproof
    - *Reading search:*
      - 2 points: full answer
      - 1 point: partial answer
    - *Other problems*: Some problems do not fit into the above categories. Unless otherwise

noted, they will be out of 4 points.
  - Axiom lists: An axiom list is a list of basic facts which are assumed to be true and which cannot be proven using a simpler list of facts. With every problem set you may also submit an axiom list. I will scan it into a PDF for my own reference. I will also give tips on which axioms are too powerful or redundant.
    - At the end of the semester I will reduce your problem set score by 5 points for each axiom which is too powerful (overkill) or redundant. (Run-on sentences may be treated as several separate axioms).
    - You receive no other points for axioms.
  - Lemma lists: It may at times be helpful to prove lemmas to help in proving your problems. You must include a list of such lemmas with your list of axioms for my reference. You receive no points for proving lemmas. For example:
    - If an axiom is removed or changed, then you will lose points for all proofs involving that axiom except:
      - (a) If you prove a lemma which proves your old assertion, then you will receive full credit for all problems involving the removed axiom.
      - (b) If you reprove the problem, your problem will be marked as late (½ points)
  - Disclaimer: problems are taken from many sources, including: Number theory through inquiry, PROMYS, A classical introduction to modern number theory, and the textbooks listed in the Basic Course Information section above.
- **Discussion forums:** on mycourses I will post a variety of discussion questions. You may get credit towards your problem set grade for *one posting per week:*
  - 4 points: a rare posting which includes one or more excellent insights
  - 3 points: provides a good contribution to the discussion and has a different subject line
  - 2 points: an o.k. posting which has a different subject line
  - 1 point: a minor posting
  - 0 points: a posting which does not contribute or negatively contributes to the discussion
- **Exams:** There will be one **midterm exam** and one **final exam**. The midterm exam will take place in the evening. Both exams have equal worth in your final grade.
  - The final exam in this class will be Tuesday May 12th, 8-11am.

Grading

This course will be graded as follows:
- 50% Problem sets
- 25% Midterm exam
- 25% Final exam

After each exam a new scale will be created specifically for that exam. In addition, a scale will be created for the problem sets, with the C cutoff equaling the number of points associated to the "Core Problems." These scales, using the weights indicated above, will be used to create the final scale at the end of the semester.

The following scale is a guideline; achieving the given score will *guarantee* the given letter grade, however the scale may be modified in favor of increasing students' letter grades

A 93-100%	A- 90-92%	B+ 87-89%	B 83-86%	B- 80-82%
C+ 77-79%	C 73-76%	C- 70-72%	B 83-86%	E 0-59
			D 60-69%	

Shorthand Feedback
In order to maximize the amount of feedback I can give on problem sets, I will use the following shorthand abbreviations:

S1: Something within your list of axioms is redundant. Please simplify it.
S2: Something within your list of axioms is too powerful (overkill). Please simplify it.
S3: You have removed an axiom from your list which you used in several problems you received credit for. Please prove the axiom using your new set of axioms.
S4: Proof missing.
S5: Citation missing.
S6: Not all variables are defined.
S7: Some variables are defined more than once.
S8: You are incorrectly using the definition.
S9: Illegible. Please resubmit the problem.
S10: There are some very minor flaws. Fix them and resubmit for full credit.

Calculators
You are welcome to use calculators in this course. They cannot prove theorems for you, but you can often use them to get experimental data which you can use to develop your intuition about a problem. However, calculators will not be allowed on exams.

Collaboration
Joint-solutions: You may submit joint problem sets with one classmate, with the following restrictions:

- You alternate writing the solutions to the problem set
- You may not switch partners during the semester, however you may stop working with a partner at any time
- Whoever is not writing the solutions is the *checker*. He or she is most responsible for ensuring that the work is correct. For this reason, I expect jointly-submitted solutions to be *better* than individually-submitted solutions.

A-students: If your aim is to get an A in the course I strongly recommend that you work mostly on your won. Problem solving skills are best mastered by practicing on your own. When working with another student, you should try your best not to look at their work. Instead, ask him or her for a tip or for the key concept which was used to solve the problem.

Citations: Most problems should be solvable without reference to other sources (except to look up definitions). You may consult other sources for ideas and intuition, but you should never copy solutions from them.

If you use any of the following to solve a problem, you should cite it:

- *Books / webpages:* if you found a great idea from a book or webpage, cite where you got it.
- *Classmates:* if you received a great idea from a classmate, cite whom you got it from. If contributions between you and your classmate were equal, say so.
- *Computer calculations*: write the code you used.

Problem Solving
Problem solving is difficult by nature. When you have difficulty solving a problem, you might try:

1) Look up the definitions. Make sure you understand them correctly.
2) Can you do part of the problem? A step? (I may give partial credit for a significant part)
3) Is it false? Can you find a counterexample?
4) Is it related to any previous problems? Maybe going back and solving an old (related) problem will be easier now.
5) Can you conjecture something similar (simpler or more general) which is true? It may help solve the problem, or it may be interesting in its own right.
6) Take a break and think about it this afternoon, or tomorrow morning.

How to Solve It by Polya has many more tips.

Special Needs
If you have any special needs (hearing impaired, handicapped, etc) that I can do anything in my class to better accommodate you, please contact me.

Questions/Concerns
If you have other questions or concerns, please see me in my office hours. Lecture time is valuable, so I would prefer do discuss your concerns outside of class.

Study Budies

1) Name: _____ E-mail / phone: _____

2) Name: _____ E-mail / phone: _____

3) Name: _____ E-mail / phone: _____

4) Name: _____ E-mail / phone: _____