Math 40520 Theory of Numbers
Fall 2015 Syllabus

Andrei Jorza

Course Website

You will find all this information as well as homeworks and other announcements on the course website:

`http://www3.nd.edu/∼ajorza/courses/2015f-m40520`

Alternatively you there is a link to this website directly from my page `http://www3.nd.edu/∼ajorza` which comes up on Google if you search my name.

Course Description

"Elementary Number Theory", our topic for the semester, traditionally covers the basic results of number theory that do not require advanced commutative algebra or complex analysis. That said, our goal for the semester is not merely to acquaint you with the classical results of number theory. Our ultimate goal is to explore the most surprising areas of this beautiful subject so as to allow you to pursue any number theory related topics you may wish in the future, whether more advanced number theory topics or applications of number theory in other areas.

Course Topics

The actual topics we will cover in the course depend in large part on your preferences and prior knowledge. I will create a more concise list once we decide on exact topics.

We will certainly cover divisibilities and congruences as they are an essential tool in number theory. As a result we will prove the existence of primitive roots and modular logarithms and perhaps an application in Elgamal encryption. We'll study the distribution of prime numbers using combinatorial methods and perhaps a little calculus. A related topic is Möbius inversion. Depending on popular demand we'll study division with remainder for more complicated integers and determined in how many ways a positive integer can be written as a sum of two squares. A related topic is that of quadratic residues and quadratic reciprocity for which we'll use exponential sums. Again, depending on popular demand, we will apply quadratic residues to encryption or some diophantine equations. We will study a number of elementary methods of solving diophantine equations including descent, which allowed Fermat to prove the only case of his last theorem that he actually did prove. We may also study some combinatorial results on quadratic forms and Gauss composition (and understand why recent Fields medalist Bhargava is famous). I would also like to explain why the Bernoulli numbers, which show up in the Taylor expansion of trig functions, are of crucial importance in number theory by computing the sum of the reciprocals of even powers of integers. Finally, depending on demand, we may explore more applied topics such as elliptic curves in cryptography or how to generate seemingly random numbers using number theory.

Policies

- Homework: There will be weekly problem sets. You are free and encouraged to collaborate with other students in the class in solving the problems, but you must write up all your solutions on your own.
- Exams: There will be a midterm exam and a final exam, both take home open book.
- Final grade: The final grade will be computed as a weighted average: 40% homework, 30% midterm, 30% final exam.

Textbook

The textbook for the course is “Elementary Number Theory” by Gareth A. Jones. For topics not included in the book I will use other (free) sources such as William Stein’s “Elementary Number Theory: Primes, Congruences, and Secrets”. I posted links on the course webpage.

Honor code

The university honor code is in effect for all your work in this course. Please refresh your knowledge of the honor code by consulting `http://honorcode.nd.edu`.

Concerns

If you have any concerns in this course please don’t hesitate to contact me `ajorza@nd.edu`, the Director of Undergraduate Studies (Sonja Mapes `smapes1@nd.edu`) or any other faculty member or adviser. It is best to address your concerns as early as possible.

Questionnaire

Please will out this questionnaire so as best to determine what topics we should cover in the class and what topics we should start with. This is not a quiz but a tool to construct the best course for you.

What do you know?

For each topic please circle what you consider is an appropriate description of your knowledge.

Rate your answer as follows:

1. Never heard of it
2. Know it exists
3. Have seen before
4. Have seen a number of times or have seens parts of
5. Familiar
6. Comfortable with
7. I can do it in my sleep

All of these topics show up in number theory and your honest answer will determine what topics are doable. Please don't consider "Never heard of it" in any way an inappropriate answer. It's better to claim that than to not understand.

Divisibilities and modular arithmetic.	1	2	3	4	5	6	7
Pythagorean triples.	1	2	3	4	5	6	7
Groups.	1	2	3	4	5	6	7
Rings and fields.	1	2	3	4	5	6	7
Ideals.	1	2	3	4	5	6	7
The Euclidean algorithm.	1	2	3	4	5	6	7
Algebraic integers.	1	2	3	4	5	6	7
Complex analysis.	1	2	3	4	5	6	7
Fourier transforms.	1	2	3	4	5	6	7
Linear algebra.	1	2	3	4	5	6	7
The Chinese Remainder Theorem.	1	2	3	4	5	6	7
Continued fractions.	1	2	3	4	5	6	7
Quadratic residues.	1	2	3	4	5	6	7
Cryptograpy.	1	2	3	4	5	6	7

What topics are you interested in?

Circle what you are most interested in, cross out the ones you are least interested in, leave unmarked the ones in the middle of your preferences.

1. Diophantine equations (Pythagorean triples, Pell's equations, Fermat's equation).
2. Gaussian integers ($a + bi$ with $a, b \in \mathbb{Z}$) and $n = x^2 + y^2$.
3. Cryptography.
4. The Riemann ζ function and Bernoulli numbers.
5. A little elliptic curves.

6. Binary quadratic forms and class groups of quadratic fields.
7. Number theory of polynomials.
8. Representing numbers by quadratic forms.
9. More combinatorial results.
10. More analytic results.

What level do you prefer?

Please select the level style you prefer:

1. I prefer more elementary topics which I can understand completely.
2. I am willing to accept some black box results as given and then see how to use them in more advanced topics.

Please select the abstraction style you prefer:

1. I prefer to see lots of explicit examples even if it means not delving deep enough in the abstract results.
2. I prefer not seeing so many examples but to delve deeper in abstract results.

Any other comments

Please let me know here of any other suggestions.