QR28: The Magic of Numbers Fall 2008 *Course Syllabus*

Contacts

Prof. Mike Hopkins mjh@math.harvard.edu Science Center 508 6-9520
Teaching Fellows:
David Roe (head) roed@math.harvard.edu Science Center 428e
Jesse Kass kass@math.harvard.edu Science Center 242b
Course Website: http://my.harvard.edu/icb/icb.do?keyword=k41788

Sections

Starting on Thursday September 18, each student will attend one of four sections a week run by the TFs. You will be asked to give your preferences using the online QR28 Sectioning page by evening on Saturday September 20. Until you have been assigned a section (early in the second week), please feel free to attend any section.

What are the aims of this course?

There are two goals in mind. The first is to introduce some of the beauty and mystery of the properties of numbers which have fascinated mathematicians for hundreds of years. We will discuss the patterns in their behavior and some surprising applications of those patterns. The second goal is to try to impart something of the mathematical mode of thought - that feeling of exploration, discovery and excitement associated with the learning and development of mathematics.

Text

The course material is covered in *The Magic of Numbers* by Gross & Harris. It is a required text and is available at the Harvard Coop. The Undergraduate Council also maintains a list of other sources for discounted and used copies of the text: http://www.crimsonreading.org/list.php?deptid=100
Several copies are available on 3-hour reserve in Cabot library.

Prerequisites

We won't assume any mathematical background except some basic high school algebra.

What topics will we cover?

- **Counting.** How many ways are there of lining up 6 boys and 9 girls so that no two boys are next to each other? How many 3-scoop ice cream sundaes can you make if there are 12 possible flavors? We'll look at systematic ways of dealing with these kinds of counting questions. Counting is also related to probability, so we'll look at that too and answer questions like: what is the chance of being dealt a straight flush in poker?
- **Arithmetic.** Imagine you live in a world where the only bills are a $13 bill and a $17 bill. Can you buy a newspaper for $1? How? We'll see that this is really an age-old question in arithmetic and we'll develop methods to answer this and other problems involving least common multiples, greatest common divisors and prime numbers. We'll introduce the powerful Euclid's Algorithm, which has been known since the time of the ancient Greeks. We'll investigate some of the beautiful and mysterious properties of prime numbers, which are the building blocks of our counting system.
- **Modular Arithmetic.** We all know the counting numbers 1,2,3,... and we know about fractions and decimals too. But what about a number system with only 7 numbers? Or 24 numbers? Does it even make sense to call this a number system? The study of these kinds of systems and their properties is called modular arithmetic. Why are these interesting? You'll see...
- **Codes and primes.** When you send your credit card information over the internet, why is that safe - even if someone is listening in? We'll learn all about sending codes and how prime numbers and modular arithmetic lie at the heart of the ingenious public-key cryptography. This is a coding system used by the internet, the banks, even the military. It can't be cracked. (At least, let's hope it can't...)

Homework

Homework assignments will be given after every lecture, and they will be due the following lecture. Yes, this sounds like a pain, but the homework assignments will be short, we promise, so it's not nearly as much work as it sounds. The reason for this policy is that it's important to keep up with the lectures and really the only way to do this is by doing a few problems after every class. Each homework assignment will be graded 0-5 points. All of the homework questions will be posted on the website (go to the *Schedule and Homework* page); they will not be handed out in class. Homework is due the lecture after it is assigned. Absolutely NO LATE HOMEWORK will be accepted, but the lowest three homework grades will be discarded at the end of the semester. Homework will be returned during the sections.
We encourage you to work together on the homework: talking to others about math really helps improve your understanding. However, the final writeups for each homework should be in your own words.

Exams

There will be two midterm examinations during the semester and a final exam during finals period. The midterms will be given during class on Wednesdays October 8 and November 12. If you have a conflict with either of the exam times, notify one of the TFs immediately. The final exam is scheduled for Friday January 16 (exam group 3) and is administered by the registrar's office.

Grading Policy

The final grade will be based on the homework, the two midterms, and the final, as follows:

- Midterm 1: 15%.
- Midterm 2: 20%.
- Final: 30%.
- Homework: 35%.

Office Hours

Professor Hopkins will hold office hours in Science Center 508, Wednesdays 2:30-3:30.
David Roe will hold office hours Friday 11-12 in the 4th floor mathematics department common room (enter the math department on the 4th floor from the elevator, and continue down the corridor), and Jesse Kass Thursday 12-1 in his office.
No appointment is necessary - just turn up if you have any questions. If you can't make that time, please do not hesitate to contact any of us at the above email addresses to arrange a meeting.

QR28: The Magic of Numbers Fall 2008 *Course Syllabus*

The following schedule is somewhat tentative and subject to change. All references are to *The Magic of Numbers* by Gross & Harris (see *Text*).

Mon	Sept 15	Introduction to QR28: The Fibonacci Sequence.
Wed	Sept 17	**Part I. Counting.** Simple counting. Chapter 1.
Fri	Sept 19	More on counting. Introduction to Probability.
Mon	Sept 22	The Multiplication principle. Chapter 2.
Wed	Sept 24	The Subtraction principle. Chapter 3.
Fri	Sept 26	How to count collections of objects. Chapter 4.
Mon	Sept 29	More on counting collections. Probability. Chapters 4 & 5.
Wed	Oct 1	Probability continued. Chapter 5.
Fri	Oct 3	Pascal's Triangle and the Binomial Theorem. Chapter 6.
Mon	Oct 6	Review.
Wed	Oct 8	**Midterm 1.**
Fri	Oct 10	**Part II. Arithmetic.** Divisibility and Euclid's Algorithm. Chapter 8.
Mon	Oct 13	*Columbus Day. University Holiday.*
Wed	Oct 15	More on Euclid's Algorithm. Chapter 8.
Fri	Oct 17	Combinations. Chapter 9.
Mon	Oct 20	Solving Diophantine equations. Chapter 9. Primes. Sections 10.1 and 10.2.
Wed	Oct 22	Prime and composite numbers. The Sieve of Eratosthenes. Chapter 10.
Fri	Oct 24	Factorization. Chapter 11.
Mon	Oct 27	Consequences of unique factorization. Chapter 12.
Wed	Oct 29	**Part III. Modular Arithmetic.** Arithmetic mod n. Chapters 14 and 15.
Fri	Oct 31	Another way to look at modular arithmetic. Chapter 16.
Mon	Nov 3	Dividing in modular arithmetic. Chapter 17.
Wed	Nov 5	Calculating powers in modular arithmetic. Chapter 18.
Fri	Nov 7	Fermat's Theorem. Calculating high powers in modular arithmetic. Chapter 18.
Mon	Nov 10	Review.
Wed	Nov 12	**Midterm 2.**
Fri	Nov 14	Computing roots in modular arithmetic. Chapter 19.
Mon	Nov 17	Chapter 19. Computing roots again.
Wed	Nov 19	Chinese Remainder Theorem.
Fri	Nov 21	More Chinese Remainder Theorem.
Mon	Nov 24	Euler's function. Chapter 13.
Wed	Nov 26	Euler's Theorem. Chapter 20.
Fri	Nov 28	*Thanksgiving Recess.*
Mon	Dec 1	**Part IV. Codes and Primes.** Types of codes. Chapter 21.
Wed	Dec 3	Public-key cryptography. Chapter 22.
Fri	Dec 5	Distribution of primes. Chapter 23.
Mon	Dec 8	How to find large primes. Chapter 23.
Wed	Dec 10	Miller-Rabin test. Generators. Chapters 23, 24.
Fri	Dec 12	Generators. Square roots of -1. Passwords. Chapter 24.
Mon	Dec 15	*No class. Happy holidays!*
TBA	Jan	Review Sessions
Fri	Jan 16	**Final Exam**