QR28: The Magic of Numbers Fall 2007 *Course Syllabus*

Contacts

Prof. Dick Gross	gross@math.harvard.edu	Science Center 506	5-9063
Prof. Joe Harris	harris@math.harvard.edu	Science Center 339	5-5335

Teaching Fellows:

Cameron Freer (head)	freer@math.harvard.edu	Science Center 242g
Rina Anno	rina@math.harvard.edu	Science Center 333c
Dawei Chen	dchen@math.harvard.edu	Science Center 426d
David Roe	roed@math.harvard.edu	Science Center 428e

Course Website: http://my.harvard.edu/icb/icb.do?keyword=k20759

Sections

Starting on Thursday September 20, each student will attend one of nine 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 22. 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 text *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/index.php?id=802

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 the 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.

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 Friday October 12 and Monday November 19. If you have a conflict with either of the exam times, notify one of the TFs immediately. The final exam is scheduled for Tuesday January 15 (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 Gross will hold office hours on Mondays 3:00 - 4:30 PM in Science Center 506. Professor Harris will hold office hours on Fridays 3:00 - 4:30 PM in Science Center 339. 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 either of them at the above email addresses to arrange a meeting.

All TF office hours will take place in the 4th floor mathematics department common room. To find it, enter the mathematics department on the 4th floor from the elevator, and continue down the corridor.

Cameron Freer	Thursday 5:00 - 6:00 PM
Rina Anno	Tuesday 3:00 - 4:00 PM
Dawei Chen	Wednesday 4:00 - 5:00 PM
David Roe	Wednesday 11:30 AM - 12:30 PM

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 17	Introduction to QR28: The Fibonacci Sequence.
Wed	Sept 19	**Part I. Counting.** Simple counting. Chapter 1.
Fri	Sept 21	The Multiplication principle. Chapter 2.
Mon	Sept 24	The Subtraction principle. Chapter 3.
Wed	Sept 26	How to count collections of objects. Chapter 4.
Fri	Sept 28	More on counting collections. Probability. Chapters 4 & 5.
Mon	Oct 1	Probability continued. Chapter 5.
Wed	Oct 3	Pascal's Triangle and the Binomial Theorem. Chapter 6.
Fri	Oct 5	Advanced topics in counting.
Mon	Oct 8	*Columbus Day. University Holiday.*
Wed	Oct 10	Review.
Fri	Oct 12	**Midterm 1.**
Mon	Oct 15	**Part II. Arithmetic.** Divisibility and Euclid's Algorithm. Chapter 8.
Wed	Oct 17	More on Euclid's Algorithm. Chapter 8.
Fri	Oct 19	Combinations. Chapter 9.
Mon	Oct 22	Solving Diophantine equations. Chapter 9. Primes. Sections 10.1 and 10.2.
Wed	Oct 24	Prime and composite numbers. The Sieve of Eratosthenes. Chapter 10.
Fri	Oct 26	Factorization. Chapter 11.
Mon	Oct 29	Consequences of unique factorization. Chapter 12.
Wed	Oct 31	**Part III. Modular Arithmetic.** Arithmetic mod *n*. Chapters 14 and 15.
Fri	Nov 2	Another way to look at modular arithmetic. Chapter 16.
Mon	Nov 5	Dividing in modular arithmetic. Chapter 17.
Wed	Nov 7	Calculating powers in modular arithmetic. Chapter 18.
Fri	Nov 9	Fermat's Theorem. Calculating high powers in modular arithmetic. Chapter 18.
Mon	Nov 12	*Veterans' Day. University Holiday.*
Wed	Nov 14	Computing roots in modular arithmetic. Chapter 19.
Fri	Nov 16	Review.
Mon	Nov 19	**Midterm 2.**
Wed	Nov 21	More on computing roots. Chapter 19.
Fri	Nov 23	*Thanksgiving Recess.*
Mon	Nov 26	Computing roots again. Chapter 19.
Wed	Nov 28	Euler's function. Chapter 13.
Fri	Nov 30	Euler's Theorem. Chapter 20.
Mon	Dec 3	**Part IV. Codes and Primes.** Types of codes. Chapter 21.
Wed	Dec 5	Public-key cryptography. Chapter 22.
Fri	Dec 7	Distribution of primes. Chapter 23.
Mon	Dec 10	How to find large primes. Chapter 23.
Wed	Dec 12	Miller-Rabin test. Generators. Chapters 23, 24.
Fri	Dec 14	Generators. Square roots of -1. Passwords. Chapter 24.
Mon	Dec 17	*No class. Happy holidays!*
TBA	Jan	Review Sessions
Tue	Jan 15	**Final Exam**