MAT215: Elementary Number Theory and Cryptography

Lecture 1

Manjil Saikia (Ahmedabad University)

"Mathematics is the queen of the sciences and number theory is the queen of mathematics.”

- Carl Friedrich Gauss

“Beauty is the first test: here is no permanent place in the world for ugly mathematics.”

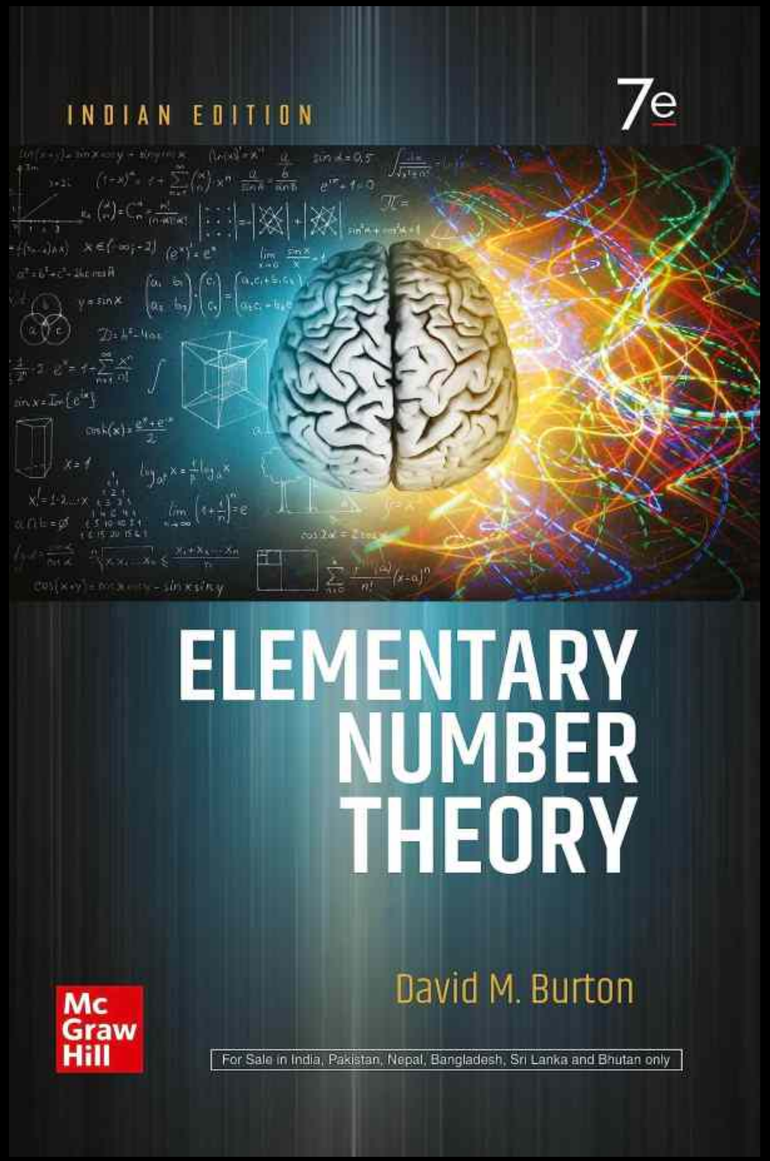
- Godfrey Harold Hardy

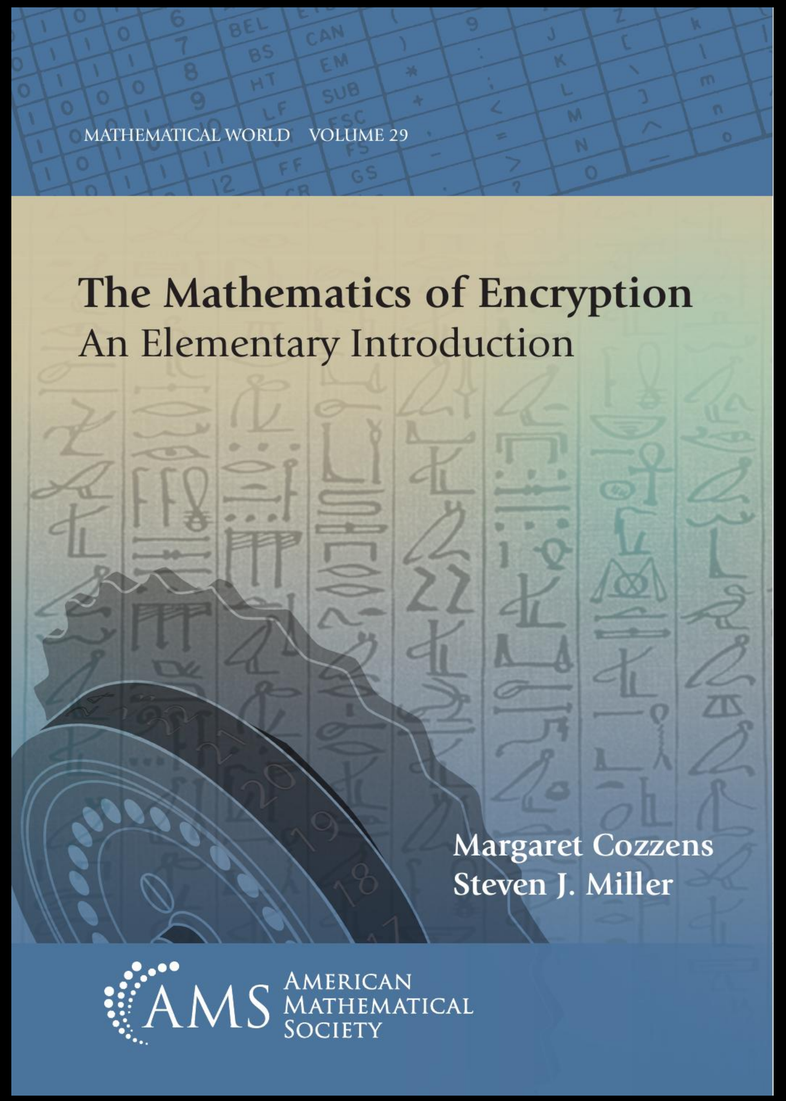
Admin

Course Details

- Largely self-contained, but it would be good to have some familiarity with mathematical proofs.
- The course will be proof-based, but with lots of examples and a little bit of history.
- Office Hours: Mondays 1100 to 1200 & Fridays 0930 to 1030 (325, SAS)
- TA: Mr Shaik Abdul Akram (M221, 2.5 Mezzanine Floor, GICT side, SAS)
- Peer Tutor: Mr Adyan Shamim
- Website: https://manjilsaikia.in/teaching/AhdUni/MAT215/
- Attendance Policy: As per University rules.

Textbooks


INDIAN EDITION
7e
ELEMENTARY NUMBER THEORY
David M. Burton
Mc Graw Hill
For Sale in India, Pakistan, Nepal, Bangladesh, Sri Lanka and Bhutan only


MATHEMATICAL WORLD VOLUME 29
The Mathematics of Encryption
An Elementary Introduction
Margaret Cozzens
Steven J. Miller
AMS
American Mathematical Society

Grading

- **Assignments (20%)**: Approximately once every week (mixture of WebWork & offline)
- **CLOSED BOOK Quiz (20%)**: Two 20-minute quizzes (Lecture 6 & Lecture 20; syllabus everything covered in Lectures 1 - 5 and Mid-Sem Exam - Lecture 19)
- **Mid-Semester Exam (20%)**: Two-hour written exam (CLOSED BOOK)
- **End-Semester Exam (20%)**: Two-hour written exam (ONE A4-sized double-sided cheat sheet allowed)
- **Project (10%)**: There will be 10 projects assigned in groups of (~#students in course)/10 students. A written report (max. 5 pages) is expected before the start of the quiet reading period.
- **Presentation (10%)**: Based on the project assigned, ideally expected before the start of the quiet reading period, duration ~ #students in group X 5 minutes.

Final Grade

- To get an A grade, a minimum 80% must be scored overall.
- This, however, doesn’t automatically guarantee an A.

Tips

- To get the most out of the course, read the textbooks assigned.
- Spend at least twice the amount we spend in lectures, on your own.
- Solve as many problems as possible.
- Meet me during office hours to discuss your progress and doubts.
- Math is collaborative, so talk to your peers as much as you can.
- Follow 3Blue1Brown and Numberphile on YouTube. Watch some of their old videos as well.

Other Details

- Do not be late for the lectures. You will be allowed ONLY two late entries during the entire semester.
- NO electronic devices in your hands during lectures, unless specifically asked to use them.
- Submission deadlines for assignments and projects will be strict. Late submissions will incur a 25% penalty per day.
- All important communications will be via email to the Course Google Group.
- All extra readings, offline assignments, slides, etc., will be posted on the course website. They will not be emailed.
- Use of AI for assignments, projects, etc. is not encouraged, but you can use AI to supplement your knowledge.

What is Number Theory?

- Deals with the properties of integers and arithmetic functions.
- One of the oldest, if not the oldest, branches of mathematics.
- Euclid studied in his Elements Books VII, VIII, and IX.
- Even earlier studied in Mesopotamia, India, China, and Egypt.
- We will just scratch the surface in this course. (Elementary means without using analysis. We will not even use abstract or linear algebra.)
- Applications are very important nowadays, and we will see basic ideas applied to cryptanalysis.
- Major figures include: Diophantus, Archimedes, Pythagoras, Pierre de Fermat, Leonhard Euler, Joseph Louis Lagrange, Adrien Marie Legendre, Carl Friedrich Gauss, Sophie Germain, Carl Gustav Jacob Jacobi, S. Ramanujan, etc.

- One reason for the endurance of number theory is that several of its problems are very easy to state, but may be very difficult to prove.
- For instance, Fermat observed that the equation $x^n + y^n = z^n$ had no solutions for $n \geq 3$ and positive integers x, y, z.
- This was proved more than 350 years later in 1990s by Andrew Wiles.
- Another instance, Goldbach observed that every even number greater than 2 can be written as the sum of two prime numbers.
- Nobody has been able to prove this assertion, although this is widely believed to be true.
- There are other problems worth $1 million. Prove them and you become very rich and very famous!

Some Motivating Examples

- All squares are either multiples of 4 or one more than a multiple of 4.
- All numbers can be written as a sum of two squares, except those that have a prime factor which is 3 more than a multiple of 4.
- Classes of numbers: congruent numbers, perfect numbers, Mersenne primes, etc.
- You have been doing a little bit of number theory every time you tell the time.

Number Theory in Nature

Periodic Cicadas are a species of insects in North America. Cicadas are well known for their long and unique life cycles. The entire population of billions of insects lies dormant in the ground for 13 or 17 years before emerging nearly simultaneously. They live above ground only for a few weeks - just enough time to mate, reproduce, and die. There are two groups of Cicadas - one that emerges every 13 years and another that emerges every 17 years.

Cicadas are most successful when they aren’t competing for resources with the other brood. The two broods of Cicadas will emerge together only every 221 years, since 13 and 17 are co-prime integers!

Time for some Number Magic

Trick 1

- Write down any 3-digit number (0 cannot be the first digit).
- Repeat the same number again. That is, if you choose 123, then write down 123123.
- I will predict their factors!

Trick 2

- Write down a 3-digit number abc, such that c<a.
- Take it reverse cba and subtract abc - cba.
- Say this is def. Now compute def + fed.
- Compare with your neighbour.

Time for two ‘Magic’ Tricks

Date/Day Prediction

- Give me your birthdate.
- This class will be able to say what day it was by the Mid-Sem Exam.

Card Trick

- Give a smallish prime number p (although the trick will work with any prime).
- Give a number less than p, say k.
- Now we do the following: take p cards from the deck, we flip up every kth card, and continue until the last face-down card is left.
- I will predict the last face-down card.

What is Cryptography?

- Another ancient subject, widely used for military purposes.
- The impetus gained momentum in the 1970s onwards due to the need for communication channels in banking.
- The transmission of online data and e-commerce boosted this requirement further.
- We will start with the Caesar Cipher and go on till RSA (at the very least).

Basic Idea

- Modern Cryptography lies at the intersection of math and CS. We will mostly focus on the math involving number theory, while there will be some digressions to CS in the later portion of the course.
- Although cryptography and codes usually bring to our mind spies, in modern times, every one of us uses them implicitly every day.
- The basic setup is: two people need to exchange information quickly, efficiently, and securely, often in the presence of an adversary who is actively snooping to intercept the information.
- For instance, online payments. First, you need to authorize your card/bank to transfer funds to the merchant. But this is not face-to-face, so you need to be sure that what you are doing is secure.
- This transfer has to be fast and error-free! (Enter analysis of algorithms, and error detection and correction codes.)

Early example of encryption: hieroglyphs on the Papyrus of Ani (~ 1250 BCE)

Polybius Checkerboard (~ 300 - 400 BCE)

- SPY would be 43 35 54.
- I/J are indistinguishable.
- Quite easy to decode, and not very secure.

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Ciphers & Codes

- A cipher is a method of concealment in which the primary unit is a letter.
- A letter is replaced by a different symbol (letter, number, etc.).
- A code is a method of concealment using words, numbers, or syllables to replace original words or phrases.
- Frequency analysis is used to break ciphers. Al-Kindi (in 750 CE), a Muslim mathematician from modern-day Iraq, was a pioneer in the area, using probability theory (800 years before it was ‘invented’ by Fermat & Pascal).
- Until the late 19th and early 20th century, cryptography did not emerge as a very technical field (in our knowledge system view).

WWII


Nur Glühlampen mit 12 mm Durchmesser verwenden


"BENEDICT CUMBERBATCH IS OUTSTANDING"
"A SUPERB THRILLER"
"THE BEST BRITISH FILM OF THE YEAR"
"AN INSTANT CLASSIC"
THE TRUE ENIGMA WAS THE MAN WHO CRACKED THE CODE
BENEDICT CUMBERBATCH
KEIRA KNIGHTLEY
THE IMITATION GAME
IN CINEMAS NOVEMBER 14

- The 1st WW was the chemist’s war, the 2nd WW was the physicist’s war, the 3rd WW is likely to be the mathematician’s war!
- Although technically not cryptography, decipherment of ancient languages is also of interest.
- The Harappan language is still not deciphered!

Hope you have fun!