MATH 4150 – Introduction to Number Theory (Spr'10)

Class location and time: Skiles 256, MWF 2-3 pm
Instructor : Prasad Tetali, office: Skiles 234, email: tetali@math.gatech.edu
Office Hours (tentative): Thurs. 2-3 pm, Fri. 4:15-5:15 pm (in Skiles 234)

Course Syllabus: Chapters 3 through 11 and 13 will be covered from the textbook, "Elementary Number Theory and its applications," (5th edition) by Kenneth H. Rosen.

Course website: http://www.math.gatech.edu/∼tetali/TEACH/Math4150.html

Outline of topics:

- Prime numbers, Unique factorization, Linear Diophantine equations
- Congruences, Chinese remainder theorem, Special congruences
- Multiplicative functions, Fermat's little theorem, Wilson's theorem
- Primality Testing: Pseudoprimes, Rabin-Miller test
- Primitive roots and Discrete logarithms
- Pollard's methods for Discrete Logarithm and Factoring
- More sophisticated : AKS Primality, Quadratic Sieve Factoring
- Quadratic reciprocity and Gauss's theorem
- Nonlinear Diophantine equations (Pythagorean triples, sums of squares)
- (done intermittently) *Cryptography Applications*: RSA cryptosystem
  El Gamal cryptosystem and signature schemes
  Zero-knowledge proofs and identification schemes
- •• (time-permitting) Elliptic Curves: the group law
- •• (time-permitting) *Elliptic curve-based and other cryptosystems*

Course Objective.

• To develop interest in various aspects of number theory, with special emphasis on i) *primitive roots*, (ii) *primality testing and factoring*, (iii) *cryptographic applications*, and somewhat ambitiously (iv) *elliptic curves*.

Guest Lecturers. On occasion we will have a guest lecturer who is an expert in number theory and/or cryptography, speaking on a subtopic of current interest.

Hand-outs. Besides the textbook, additional material from various sources will be distributed throught the semester.

Testing. There will be TWO tests and an (all-inclusive) FINAL exam, all in-class.
Homeworks will be assigned, collected and graded on a regular basis. *Can work together, but must write your own solutions.*
Assessment. Homeworks : 15%; Each Test : 25%; FINAL exam : 35%
• **Test 1** : **February 12th** (Friday); **Test 2** : **April 2nd** (Friday)
NO MAKE-UPs, please!

• **Important Tips**: Feel free to ask questions any time! Make use of office hours!! Feel free to provide *feedback during the course*, and not wait until the end of the term, but *please do complete the online survey at the end of the term* !!!

SPRING 2010: MATH 4150 (Intro to Number Theory) : Prasad Tetali

---

- Class time and location : MWF 2-3 pm ; Skiles 256
- Office : Skiles 234 ; Email: tetali@math.gatech.edu
- Office hours: Thurs. 3-4pm, Fri. 4:15-5:15 (in Skiles 234);
  Also available Monday 12-1:30 (in Klaus 2115), and drop-in or appt. are both encouraged!

- Click here for an outline of the course
- Click here for an excerpt from Thomas Koshy's book, showing a formula for the GCD of two integers
- TEST 2 is posted here: (Take-home extension until Tuesday NOON):
- TEST 1 - Make up (for those missed due to inclement weather) is posted here: (Make-up to Test 1):
- TEST 1 is posted here: (Original Test 1)
- **PLEASE FILL OUT Course-Instructor Opinion Survey** : available at (Course Evaluation)

  - **FINAL EXAM:** **In Skiles 256 on May 7th (8:00am -- 10:50 am) : closed book, closed notes; TWO Sheets of Info. allowed, simple calculators allowed.**
  - **HOMEWORKS:** ** SOLUTIONS POSTED ON T-SQUARE **

    - **Homework 7 (No need to submit; for practice only)**
      Section 11.2 : Problems 1 (c,d), 3, 6, 11
      Section 11.3 : Problems 1 (c,d), 3, 9, 10
      Section 13.1 : Problems 6, 15, 18
      Section 13.2 : Problems 2, 3, 4, 5, 7
    - Homework 6 (Due on Wednesday, April 21st)
      Section 9.3: Problems 13, 14
      Section 9.4: Problems 8, 9, 10
      Section 9.6: Problems 5, 8, 9
      Section 11.1: Problems 5, 10, 19, 28 (b), 33, 34
    - Homework 5 (*No need to submit* will discuss in class on Wednesday, 3/31)
      Section 9.1: 3, 8, 9, 10, 15
      Section 9.2: 7, 9, 10, 11, 13
    - Homework 4 (Due: Wednesday, March 17th)
      Section 6.3 : 3, 6, 10, 15
      Section 7.1 : 19, 25, 31, 32, 42
      Section 7.4 : 17, 21, 22, 28

      Optional Problems:
      Section 6.3 : 2, 7
      Section 7.1 : 40, 41, 44, 52
      Section 7.4 : 9, 27, 30
    - Homework 3 (Due: Monday, March 1st)
      Section 6.1: Problems 14, 15, 17, 21, 25, 26, 33
      Section 6.2: Problems 2, 7, 9, 10, 18, 20

      Optional Problems: Section 6.1: 5, 25, 39, 49

Optional Problems: Section 6.1: 5, 25, 39, 49
Section 6.2 : 5, 6, 17

- Homework 2 (*Due: Monday, Feb. 8th*)
  Section 3.4 : Problems 2(d), 4(d)
  Section 3.5 : Problems 10, 19, 20, 34, 48
  Section 3.7 : Problems 6, 9, 14(a)

  Optional problems (no need to submit):
  Section 3.5: 9, 29, 33; Section 3.7: 3, 7, 13.

- Homework 1 (***Due: Wednesday, Jan. 27th***)
  Section 3.1 : Computational Exercise 7
  Section 3.2 : Problem 3
  Section 3.3 : Problems 14, 15, 21, 22
  Section 4.1 : Problems 14, 15, 21, 22