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* !!!