MAT 514: Theory of Numbers independent study (Fall 2012)

Course number: MAT 514

Course title: Theory of Numbers independent study (Fall 2012)

Credits: 3

Prerequisites: Permission of instructor.

Instructor information:

Instructor: Dr. Dan Yasaki `d_yasaki@uncg.edu`
Homepage: `http://www.uncg.edu/math/faculty/d_yasaki/teaching.html`
Office Hours (146 Petty): Mondays 8:30 - 9:30 AM, Tuesdays & Thursdays 11:00 - noon

For whom planned: Abhishek Pratap

Catalog description: An introductory course to both multiplicative and additive number theory. Divisibility, prime numbers, congruencies, linear and nonlinear Diophantine equations (including Pell's equation), quadratic residues, number-theoretic functions, and other topics.

Student learning outcomes: Upon successful completion of this course, students will be able to:

- define the fundamental terms in elementary number theory.
- explain how RSA encryption allows for secure message transcription.
- combine definitions and results to create rigorous proofs of basic statements about elementary number theory.
- evaluate an argument for logical validity.

Teaching methods and assignments for achieving learning outcomes: The student will read and work through the course material independently. Achievement of learning outcomes will be facilitated via homework assignments/weekly presentations by the student and the final exam.

Evaluation and grading: Semester averages are rounded to the nearest point, and letter grades are assigned on a 10 point scale.

A+ : 97–100	B+ : 87–89	C+ : 77–79	D+ : 67–69	
A : 93–96	B : 83–86	C : 73–76	D : 63–66	F : 0 – 59
A− : 90–92	B− : 80–82	C− : 70–72	D− : 60–62	

- Weekly homework presentations (70%)
- Final exam (30%)

Required text:

- Textbook: *Elementary Number Theory: Primes, Congruences, and Secrets* available at `http://wstein.org/ent/`

Topical outline:

- Divisibility and greatest common divisors
- Modular arithmetic
- Prime numbers and uniques factorization
- Primitive roots
- Diffie-Helman key exchange
- Chinese remainder theorem
- Euler's formula
- Diophantine equations
- RSA public key cryptosystem
- Factorization techniques
- Quadratic residues and quadratic reciprocity
- Additional topics such as elliptic curve cryptography if time permits.

Academic Integrity Policy: Each student is required to sign the Academic Integrity Policy on all major work submitted for the course.

I have abided by the UNCG Academic Integrity Policy on this assignment.
Signature _____ Date _____

More information can be found at `http://academicintegrity.uncg.edu/complete/`.

Final examination: The Final Exam covers the entire semester. The time and date will be announced later in the semester.