

## CMPSC/MATH 467 Factorization and Primality Testing

Catalog Data: Factorization and Primality Testing (3)  
Prime sieves, factoring, computer numeration systems, congruences, multiplicative functions, primitive roots, cryptography, quadratic residues. Students who have passed MATH 465 may not schedule this course. Prerequisite: CMPSC 360 or MATH 311W.

Typical Textbook: *Factorization and Primality Testing* by David M. Bressoud, Springer-Verlag, 1989, ISBN 0-387-97040-1.

**Supplemental Textbooks – not required:**

*Cryptanalysis of Number Theoretic Ciphers* by Samuel S. Wagstaff, Jr, Chapman & Hall/CRC, 2003, ISBN 1-58488-153-4.

*Primality Testing and Integer Factorization in Public-Key Cryptography* by Song Y. Yan, Kluwer Acad. Pub., 2004, ISBN 1-4020-7649-5

*Prime Numbers*, by R. Crandall & C. Pomerance, Springer, 2<sup>nd</sup> Ed., 2005, ISBN 0-387-28252-7 This is a great book that covers an amazing amount of material at a somewhat more advanced level.

Course Objectives: The purpose of this course is to introduce students to an active, important, and fascinating interface between number theory and computer science.

We will see how the seemingly simple, and certainly basic, notion of decomposition of integers into products plays a vital role in some important modern computer security schemes. We will investigate the relationship between the reliability of these schemes and the ease with which factorization can be carried out.

That will lead us to consider powerful factorization techniques which are only a generation or so behind the present state of the art (which itself is beyond the level of this course, but which builds on what we will be doing in an absolutely essential way).

Primary Course Outcomes:

Relationship to Undergraduate  
Program Outcomes:

Required Topics:

- Unique Factorization, Euclidean Algorithm, and Sieving
- Perfect Numbers and Euler's Generalization of Fermat's Theorem
- RSA Public Key Crypto-System
- Preliminary Factorization Techniques
- Strong Pseudoprimes, Quadratic Residues, and Quadratic Reciprocity
- The Quadratic Sieve
- Primality Testing
- Groups and Elliptic Curves
- Elliptic Curves, Factorization, and Primality Testing

Class Format: Three lectures per week.

Professional Component:

Evaluation: Except for the first week, we will have homework assigned on Friday and due the next Friday. The homework will consist partly of **proofs** and partly of machine **implementation of algorithms**, which must be amply explained. At the end of the semester, after the last homework is due, we will have easy daily 5-point quizzes on the material presented that day.

The homework and final quizzes will be worth 100 points, the midterms will be worth 100 points each, and a final factorization project will be worth 100 points.

Author: W. D. Brownawell, MATH  
Last Revised: October 9, 2007