

Module Syllabus:

Course Title: Computational Number Theory
 Course Code: 250472
 Semester: Second 2009/2010
 Lecturer : Amin Witno
 Office Room: 820 (Ext. 2228)
 Office Hours: STR 10–11; MW 11–12
 E-mail: awitno@gmail.com

Short Description:

This module discusses the computational aspect of elementary number theory, focusing on two main research topics in the area: factorization and primality testing. Public-key cryptography is introduced as a motivational background which also provides contextual applications and examples.

Topics by the Week:

Week	Dates	Topics
1	22/02 – 25/02	The Theory of Divisibility, Prime Numbers and Congruences, Wilson's Theorem
2	28/02 – 04/03	The Chinese Remainder Theorem, Fermat's Little Theorem, Euler Phi-Function
3	07/03 – 11/03	Modular Exponentiation, Successive Squaring Algorithm, The RSA Cryptosystem
4	14/03 – 18/03	Attacks on the RSA, Primitive Roots
5	21/03 – 25/03	Quadratic Reciprocity
6	28/03 – 01/04	Divisibility Tests, Fermat Factorization, Pollard's Rho Method
7	04/04 – 08/04	Pollard p-1 Method, Exponent Factorization, Quadratic Sieve
8	11/04 – 15/04	Continued Fractions, Periodic Continued Fractions
9	18/04 – 22/04	Factorization using Continued Fractions
10	25/04 – 29/04	Pseudoprimes, Carmichael Numbers, Korselt's Criterion
11	02/05 – 06/05	Miller-Rabin Test, Strong Pseudoprimes, Rabin's Probabilistic Test
12	09/05 – 13/05	Lucas' Converse of Fermat's Little Theorem, Pocklington's Test, Proth's Test
13	16/05 – 20/05	Lucas Sequences, Primality Criteria
14	23/05 – 27/05	Fermat Numbers, Mersenne Primes and Perfect Numbers
15	30/05 – 03/06	Review for Final Exam
16	07/06 – 15/06	Final Exam will be held in this period

Mark Distribution:

- Exam 1 31/03/2010 20%
- Exam 2 05/05/2010 20%
- Project TBA 10%
- Final Exam TBA 50%

References:

- Bressoud and Wagon, A Course in Computational Number Theory, Springer 2000
- Kenneth Rosen, Elementary Number Theory and Its Applications, Addison Wesley 2005
- Amin Witno, Theory of Numbers, BookSurge Publishing 2008

Course Notes:

- Computational Number Theory, required and is available for free at Amin Witno Web
- Number Theory, for references, also free from Amin Witno Web

Websites:

- Basic Sciences Department- <http://www.philadelphia.edu.jo/math>
- Amin Witno Web- <http://www.witno.com/>
- Number Theory Web- <http://www.numbertheory.org/>