Department of Basic Sciences – Philadelphia University

Module Syllabus:

Course Title:	Computational Number Theory
Course Code:	250472
Semester:	First / 2010–2011
Lecturer :	Amin Witno
Office Room:	820 (Ext. 2228)
Office Hours:	SMTWR 11–12
E-mail:	awitno@gmail.com

Short Description:

This module deals with the computational aspects of elementary number theory, focusing on two main research topics: 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	Topics
1	The Theory of Divisibility, Prime Numbers and Congruences, Wilson's Theorem
2	The Chinese Remainder Theorem, Fermat's Little Theorem, Euler Phi-Function
3	Modular Exponentiation, Successive Squaring Algorithm, The RSA Cryptosystem
4	Attacks on the RSA, Primitive Roots
5	Quadratic Reciprocity
6	Divisibility Tests, Fermat Factorization, Pollard's Rho Method
7	Pollard p-1 Method, Exponent Factorization, Quadratic Sieve
8	Continued Fractions, Periodic Continued Fractions
9	Factorization using Continued Fractions
10	Pseudoprimes, Carmichael Numbers, Korselt's Criterion
11	Miller-Rabin Test, Strong Pseudoprimes, Rabin's Probabilistic Test
12	Lucas' Converse of Fermat's Little Theorem, Pocklington's Test, Proth's Test
13	Lucas Sequences, Primality Criteria
14	Fermat Numbers, Mersenne Primes and Perfect Numbers
15	Review for Final Exam
16	Final Exam will be held in this period

Mark Distribution:

Exam 1	14/11/2010	20%
Exam 2	14/12/2010	20%
Project	TBA	10%
Final Exam	TBA	50%

Course Notes:

My lecture notes, Computational Number Theory, are required and available for free download from the web site: http://www.philadelphia.edu.jo/math/witno/notes.htm

Textbook:

No textbook is required. A recommended text is the one I have written, Theory of Numbers, BookSurge Publishing 2008. A more excellent book, and more pricely, is David Bressoud's Factorization and Primality Testing, Springer 1980.

Web sites:

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