Module Syllabus:

Course Title: Number Theory
Course Code: 250313
Semester: First / 2014–2015
Lecturer : Amin Witno
Office Room: 820 (Ext. 2228)
Office Hours: SUN/TUE/THU 10–11 & MON/WED 11–12
E-mail: awitno@gmail.com

Short Description:

This module is an introduction to elementary number theory, covering the basic theory of divisibility, prime numbers, and congruences, with selected applications in cryptography.

Week-by-Week Plan:

Week	Topics of Study
1	A survey into number theory, divisibility, residues, GCD.
2	Euclidean algorithm, Bezout's lemma, extended Euclidean algorithm, solving linear equations. Project: Divisibility Criteria
3	Primes, trial division, factorization, the fundamental theorem of Arithmetic, evaluating GCD using factorization.
4	The infinitude of primes, the prime number theorem, Dirichlet's theorem, well-known conjectures concerning prime numbers. Project: Factorization Methods
5	Congruences, complete residue systems, solving linear congruences, modular inverses.
6	Wilson's theorem, Chinese remainder theorem, systems of congruences. Project: Sums of Two Squares
7	Fermat's little theorem, reduced residue systems, the Euler's phi-function.
8	Euler's theorem, evaluating the phi-function and large powers.
9	Project: The RSA Cryptosystem
10	Orders, primitive roots, the existence of primitive roots modulo primes.
11	The primitive root theorem, solving discrete logarithm problems. Project: Secret Key Exchange
12	Quadratic residues and nonresidues, the Legendre symbol, Euler's criterion.
13	Gauss's lemma, the quadratic reciprocity law, the Jacobi symbol.
14	Computing modular square roots. Project: Electronic Coin Tossing
15	Review for Final Exam.
16	Final Exam will be held in this period.

Required Textbook:

Amin Witno, Theory of Numbers, BookSurge Publishing 2008. Students are required to download softcopies of the text for free from http://www.witno.com/numbers. Optional hardcopies are available for purchase from Amazon.com.

Lecture Notes:

Amin Witno, The Primitive Root Theorem. These optional notes are a supplement to Chapter 5 and can be downloaded for free from the course website.

Homework Assignment:

Chapter	Assigned Exercises for Homework	Extra Problems
1	1, 2, 3, 4, 6, 7, 9, 10, 11, 12, 13, 15, 18, 21, 22, 23, 24	16, 20, 25
2	1, 2, 4, 5, 7, 8, 11	6, 9, 13, 14
3	1, 2, 6, 8, 9, 10, 11, 12, 13, 19, 21, 23	3, 14, 15, 20
4	1, 3, 5, 7, 8, 12, 13, 20, 23	2, 4, 6, 9
5	1, 2, 3, 6, 7, 11, 13, 17, 19	4, 9, 15, 16, 18
6	1, 4, 6, 7, 8, 13, 17, 22	2, 9, 11, 14, 15

Mark Distribution:

- Homework 6 Sets 10%
- Quizzes 2 Sets 10%
- Exam 1 Week 6 20%
- Exam 2 Week 11 20%
- Final Exam Week 16 40%

Exam dates, once determined, will be posted online at the Department's website.

Supporting Websites:

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