

Module Syllabus:

Course Title: Number Theory
 Course Code: 250313
 Semester: Second 2011/2012
 Lecturer : Amin Witno
 Office Room: 820 (Ext. 2228)
 Office Hours: Sunday – Thursday 12–1
 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.

Textbook:

Amin Witno, Theory of Numbers, BookSurge Publishing 2008--this text is available for purchase from Amazon.com and for free download from <http://www.witno.com/numbers>.

Expected Workload:

Following the text, exercises will be assigned and graded every week. Two written quizzes and three exams will be administered during the semester. The table below lists the problem set for each chapter, in conjunction with the approximate timing and coverage of the two quizzes and three exams.

Chapter	Assigned Exercises for Home work	Extra Problems
1	1, 2, 3, 4, 6, 7, 9, 10, 11, 12, 13, 15, 18, 21, 22, 23, 24, 25	16, 20
	First Quiz – TBA/02/2012	
2	1, 2, 4, 5, 6, 7, 8	9, 13, 14
3	1, 2, 6, 8, 9, 10, 11, 12, 13, 19, 20, 21, 23	3, 14, 15
	First Exam – 13/03/2012	
4	1, 2, 3, 4, 5, 7, 8, 12, 13	6, 9
	Second Quiz – TBA/04/2012	
5	1, 2, 3, 4, 6, 7, 8, 9, 11, 13, 17, 19	10, 15, 16, 18
	Second Exam – 24/04/2012	
6	1, 4, 6, 8, 10, 11, 13, 16, 17, 18, 20, 21, 22	2, 9, 14, 15
	Final Exam – TBA/06/2012	

Mark Distribution:

- Exam 1 20 %
- Exam 2 20 %
- Quiz 1 05 %
- Quiz 2 05 %
- Homework 10 %
- Final Exam 40 %

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>