Department of Mathematics—Philadelphia University

Course Syllabus

Course Title	Number Theory
Course Code	250313
Semester	Second/2022–2023
Lecturer	Amin Witno
Office Room	814 Faculty of Science
Office Hours	Sun/Tue: 09:30–11:00; Mon/Wed: 11:00–12:30
E-mail	awitno@philadelphia.edu.jo

Short Description

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

Topics by the Week

1. A survey into number theory, basic theorems of divisibility, residues, and the greatest common divisor (GCD) function.
2. The Euclidean algorithm, Bezout's lemma, the extended Euclidean algorithm and its application in solving linear equations.
3. Primes, trial division, factoring a composite into prime numbers, the fundamental theorem of arithmetic, evaluating GCD via factorization.
4. The infinitude of primes, the prime number theorem, Dirichlet's theorem and some well-known conjectures concerning prime numbers.
5. Congruences, residue classes and complete residue systems, solving linear congruences, modular inverse.
6. Wilson's theorem, the Chinese remainder theorem, solving a system of linear congruences.
7. Fermat's little theorem, reduced residue systems and the Euler's phi-function.
8. Euler's theorem, evaluation of the phi-function, computing power mod and the successive squaring algorithm.
9. Computing root mod, the RSA cryptosystem.
10. Orders and primitive roots, the existence of primitive roots modulo primes.
11. The primitive root theorem, solving discrete logarithm problems.
12. Quadratic residues and non-residues, the Legendre symbol, Euler's criterion.
13. The quadratic reciprocity law and its proof.
14. Evaluation of the Legendre symbol using the Jacobi symbol, computing modular square roots.

Recommended Textbook

Theory of Numbers (2008) BookSurge Publishing.

The pdf version of the chapters can be downloaded free of charge at the following site.

http://witno.com/numbers

Supporting Material

There are three revision notes relevant to this course:

1. *Number Theory,* main lecture notes and exercise sets.
2. *The Primitive Root Theorem,* to supplement Chapter 5.
3. *The Quadratic Reciprocity Law,* to supplement Chapter 6.

The above materials can be obtained via the link below.

https://www.philadelphia.edu.jo/academics/awitno

Online Resources

The following shortcut will take you to my web homepage at the University, where you find the course syllabus, exam dates, copies of old exams, links to the above materials, and any important announcement related to the current semester.

http://phi.witno.com

Grade Distribution

The following guideline is tentative; it may be modified as necessary according to the University directive for the current semester.

Homeworks Quizzes Class participation	30%
Midterm Exam	30%
Final Exam	40%

Exam Dates

Exam dates, once determined, will be posted online at the homepage as well as at the University student-portal page.

Homework Exercises

Homework exercises with check answers have been uploaded to the Moodle coursepage as well as at the MicroSoft Teams channel.

AW230228