



Course Information

| | |
|-----------------------------------|--|
| Course Code | 2360365 |
| Course Section | 1 |
| Course Title | ELEMENTARY NUMBER THEORY I |
| Course Credit | 3 |
| Course ECTS | 6.0 |
| Course Catalog Description | Divisibility, congruences, Euler, Chinese Remainder and Wilson's Theorems. Arithmetical functions. Primitive roots. Quadratic residues and quadratic reciprocity. Diophantine equations. |
| Prerequisites | No prerequisites |
| Schedule | Tuesday , 13:40 - 15:30, M103 Thursday , 10:40 - 11:30, M103 |

Instructor Information

| | |
|-----------------------|--|
| Name/Title | Assoc.Prof.Dr. TOLGA KARAYAYLA |
| Office Address | M-222 |
| Email | tkarayay@metu.edu.tr |
| Office Phone | 210 5362 |
| Office Hours | To be announced |

Course Objectives

This is a basic number theory course which deals with division algorithm, prime numbers and their primitive roots, the theory of congruences, quadratic reciprocity law and number theoretic functions.

Course Learning Outcomes

The students who succeeds in this course

- will be able to use the division algorithm,
- will be able to comprehend the prime numbers, their distribution and the notion of congruence,
- will be able to define number-theoretic functions and understand their nice applications in cryptography,
- will be able to identify primitive roots and indices.

Instructional Methods

Lectures, in class discussions, exercise problems.

Tentative Weekly Outline

| Week | Topic | Relevant Reading | Assignments |
|------|---|------------------|-------------|
| 1 | The Division Algorithm, The Greatest Common Divisor. | | |
| 2 | The Euclidean Algorithm, The Diophantine Equation $ax+by=c$. | | |
| 3 | The Fundamental Theorem of Arithmetic, Primes and Their Distribution. | | |
| 4 | Basic Properties of Congruences, Special Divisibility Tests. | | |
| 5 | Linear Congruences, Chinese Remainder Theorem. | | |
| 6 | Fermat's and Wilson's Theorems. | | |



| Week | Topic | Relevant Reading | Assignments |
|------|--|------------------|-------------|
| 7 | Number-Theoretic Functions tau and sigma. | | |
| 8 | The Mobius Inversion Formula | | |
| 9 | The Greatest Integer Function | | |
| 10 | Euler's phi-Function, Euler's Theorem. | | |
| 11 | Properties of phi-Function, An Application to Cryptography | | |
| 12 | Primitive Roots. | | |
| 13 | The Quadratic Reciprocity Law. | | |

Course Textbook(s)

David M. Burton - Elementary Number Theory

Assessment of Student Learning

| Assessment | Dates or deadlines |
|--|---|
| Midterm 1 | Week 7 or 8 |
| Midterm 2 | Week 11 or 12 |
| Final Exam | Date to be announced by Student Affairs Office. |
| Quizzes in class (Bonus) Several (at least 4) quizzes will be given in class throughout the semester. Each quiz will be 10-15 minutes long. | Dates will not be announced. |
| Attendance: 5 points bonus will be given to the students who attend at least 85% of the classes. Students who attend less than 70% of the classes will be given NA (Not Attended) grade. | Attendance will be taken in all classes. |

Course Grading

| Deliverable | Grade Points |
|-------------|--------------|
| Midterm 1 | 30 |
| Midterm 2 | 30 |
| Final | 40 |



| Deliverable | Grade Points |
|--|--------------|
| Quizzes (Bonus) | 7 |
| Attendance Bonus (for attending at least 85% of classes) | 5 |
| Total | 112 |

Course Policies

Class Attendance

The students whose class attendance is less than 70% of all classes at the end of the semester will be given NA letter grade and they will fail the course. The students who are given NA grade cannot take the Final Exam. Attendance will be taken in all classes.

Students are required to attend the class on time.

Make up for Exams and Assignments

Students who have acceptable and documented reasons for missing an exam will be given a make up exam 2-3 days after the final exam. A student can take a make up exam for only one missed exam. Make up exam will cover all topics of the course.

Information for Students with Disabilities

To obtain disability related academic adjustments and/or auxiliary aids, students with disabilities must contact the course instructor and the ODTÜ Disability Support Office as soon as possible. If you need any accommodation for this course because of your disabling condition, please contact me. For detailed information, please visit the website of Disability Support Office: <http://engelsiz.metu.edu.tr/>

Academic Honesty

The METU Honour Code is as follows: *"Every member of METU community adopts the following honour code as one of the core principles of academic life and strives to develop an academic environment where continuous adherence to this code is promoted. The members of the METU community are reliable, responsible and honourable people who embrace only the success and recognition they deserve, and act with integrity in their use, evaluation and presentation of facts, data and documents."*