Linnæus University

Jnr: 2014/3187-3.1.2

Course syllabus

Faculty of Technology
Department of Mathematics

2MA406 Elementär talteori, 7,5 högskolepoäng
Elementary number theory, 7.5 credits

Main field of study
Mathematics

Subject Group
Mathematics

Level of classification
First Level

Progression
G2F

Date of Ratification
Approved by Faculty of Technology 2014-10-03
The course syllabus is valid from autumn semester 2015

Prerequisites
60 credits in Mathematics or Mathematics education including 1MA403 Vector geometry and 1MA162 Discrete Mathematics 7.5 credits or the equivalent.

Objectives
The student should know how to:

- define the basic concepts of elementary number theory
- explain and derive fundamental properties of the integers
- use the arithmetic functions to describe number theoretical relations
- solve linear congruence equations and decide if a quadratic congruence equation has a solution
- use discrete logarithms (index arithmetic)
- use methods from number theory in applications, for example cryptography
- tell about the results and applications of number theory to non-experts, for example pupils in secondary school.

Content
The course covers the following topics:

- Divisors, prime numbers and greatest common divisor. The fundamental theorem of arithmetic. Euclidean algorithm. Representation of integers in different bases.
- Arithmetic functions och Möbius inversion formula.
- Congruence. Linear congruence. The Chinese remainder theorem. The theorems of Fermat and Euler.
- Character chippers. Block ciphers. Public key cryptography especially the RSA

cryptosystem.
- Quadratic residues. The Legendre symbol. The law of quadratic reciprocity.
- Primitive roots. Index arithmetic. Random number generators. ElGamal cryptosystem.

Type of Instruction
Lectures and seminars. Compulsory assignments may be given during the course.

Examination
The course is assessed with the grades A, B, C, D, E, Fx or F.
The grade A constitutes the highest grade on the scale and the remaining grades follow in descending order where the grade E is the lowest grade on the scale that will result in a pass. The grade F means that the student's performance is assessed as fail (i.e. received the grade F).

The student's knowledge is assessed in the form of oral and/or written examinations. The principal assessment method for the course is determined at the beginning of the course.

Course Evaluation
A course evaluation will be carried out at the end of the course in accordance with the guidelines of the University. The result of the course evaluation will be filed at the department.

Credit Overlap
This course cannot be part of a degree in combination with another course in which the content fully or partly correspond to the content of this course: 2MA106
Elementary number theory, 7.5 credits

Other
Grade criteria for the A–F scale are communicated to the student through a special document. The student is to be informed about the grade criteria for the course by the start of the course at the latest.

Required Reading and Additional Study Material
Required reading
Rosen K H, *Elemenatry Number Theory and its Applications*, Pearson Addision Wesley,latest edition. 454 (721) pages.