



## Course syllabus

Faculty of Technology

Department of Mathematics

2MA406 Elementär talteori, 7,5 högskolepoäng

2MA406 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 2014-10-03

Revised 2019-03-13 by Faculty of Technology. Examination and assessment methods are revised.

The course syllabus is valid from spring semester 2020

### **Prerequisites**

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

## Objectives

After completing the course, the student should be able to

- solve problems, perform calculations, and conduct lines of reasoning within the part of mathematics that is covered by the course, and to communicate these solutions, calculations, and reasonings in writing
- describe definitions, and formulate and prove theorems that are central to the course.

## 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.

## 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 a written/oral exam.

## Course Evaluation

During the course or in close connection to the course, a course evaluation is to be carried out. The result and analysis of the course evaluation are to be communicated to the students who have taken the course and to the students who are to participate in the course the next time it is offered. The course evaluation is carried out anonymously. The compiled report will be filed at the Faculty.

## Credit Overlap

The course cannot be included in a degree along with the following course/courses of which the content fully, or partly, corresponds 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, *Elementary Number Theory and its Applications*, Pearson Addison Wesley, latest edition. 454 (721) pages.