Discrete Mathematics

Syllabus Number 2B205
Basic Major Subjects
Elective 2 credit
WATANABE, Ryuji

1. Course Description

This course provides an introduction to the algebraic system, finite field and number theory. The items are as follows: Operation and algebraic system, semi group and group, ring and field, transmission of information, error of codes, detection and correction of errors, finite field, Hamming code, cyclic code, BCH code, cryptosystem, integer, prime number and factorization into prime factors, Euclidean algorithm, diophantine linear equation, congruent expression, Fermat's little theorem, and the RSA cryptosystem.

The classes are based on self-learning to read the designated text books and to answer the practice exercises prepared in each unit of the guidance book.

This subject is related to the clause 2 of the diploma policy of the Department of Information Science Correspondence Course.

2. Course Objectives

The objectives of this course for students are to understand the basic concept of error correcting codes on the basis of finite field and the basic concept of the RSA cryptosystem which is one of the public key cryptosystems based on number theory.

3. Grading Policy

The acceptance line is accuracy rate of 60% in the final exam.
The midterm papers(40%) and the final exam (60%) will be evaluated.

4. Textbook and Reference

Textbook
F.Terada, N.Nakamura, T.Syakushi and T.Matsui "Basics of Information Mathematics" Saiensu-Sha (1999) in Japanese. (ISBN 4-7819-0914-0)
Reference
H.Ogura, T.Takahama "Introduction to Mathematical Logic in Information Science" Kindaikagakusha (1991) in Japanese. (ISBN 9784764901803)

5. Requirements(Assignments)

Answering the practice exercises prepared in each unit of the guidance book is required as the midterm papers.

Preparation of numbers, expressions and operations and characteristics of integers on a high school level and introductory linear algebra is also required.

6. Note

The assignments should be prepared by handwriting.
It is prohibited for students to refer the textbook and notebook in the final exam.

7. Schedule

[1] Algebraic system : Operation and algebraic system, Semi group and group
[2] Algebraic system : Permutation group, Cyclic group
[3] Algebraic system : Ring and field
[4] Finite field and code : Transmission of information, Error of codes
[5] Finite field and code : Detection and correction of errors
[6] Finite field and code : Finite field
[7] Finite field and code : Hamming code
[8] Finite field and code : Cyclic code
[9] Finite field and code : BCH code
[10] Number theory and cryptosystem : Cryptosystem, Integer, Prime number and factorization into prime factors
[11] Number theory and cryptosystem : Euclidean algorithm
[12] Number theory and cryptosystem : Diophantine linear equation
[13] Number theory and cryptosystem : Congruent expression
[14] Number theory and cryptosystem : Fermat's little theorem
[15] Number theory and cryptosystem : The RSA cryptosystem