2021학년도 제2학기 (온라인)강의계획안

교과목명 Course Title	정수론	학수번호-분반 Course No.	20454-01
개설전공 Department/Major	수학과	학점/시간 Credit/Hours	3/3
수업시간/강의실 Class Time/Classroom	월: 5교시, 수: 4교시 (비대면 수업 가능)		
담당교원 Instructor	성명: 이향숙 Name: Hyang-Sook Lee	소속: 수학과 Department: Mathematics	
	E-mail: hsl@ewha.ac.kr	연락처: 3277-2591	
면담시간/장소 Office Hours & Location	시간: by appointment [온라인 Zoom 이용]		

Ⅰ. 교과목 정보 Course Overview

1. 교과목 개요 Course Description

정수론은 정수의 다양한 성질을 연구하는 학문으로서, 독일의 수학자 가우스(Gauss)는 '수학은 과학의 여왕이고 정수론은 수학의 여왕이다.' 라고 할 정도로 고대 때부터 수학의 중심에 위치해 왔다. 특히, 정수론의 다양한 이론이 현대 암호 및 코딩 이론 등의 응용 학문 발전에 큰 기여를 하면서 그 중요성이 더욱 강조되어 왔다.

이 수업에서 다루는 수론의 기초 내용은 소수의 특성, 디오판틴 방정식, 산술의 기본정리, GCD, Euclidean 정리, 합동, 중국인 나머지 정리, 페르마 정리, 오일러 정리, 원시근 등이며 기초 이론에 기반한 응용으로써 고전 암호와 현대 대표적인 공개키 암호인 RSA 암호 등을 다룬다.

2. 선수학습사항 Prerequisites

없음

3. 강의방식 Course Format

강의 Lecture	발표/토론 Discussion/Presentation	실험/실습 Experiment/Practicum	현장실습 Field Study	기타 Other
100 %	%	%		%

강의 진행 방식 (course format): Laptop 사용한 판서 중심의 강의

4. 교과목표 Course Objectives

- 소수(prime) 및 정수의 다양한 특성과 성질을 배운다.
- 수론의 기본 정의 및 성질에 관한 지식을 함양한다.
- 추상적 증명을 작성하는 과정을 통해 사고하고 사유하는 능력을 키운다.
- 수론의 이해에 기반한 암호 응용을 통해 원리를 적용하여 문제를 해결하는 역량을 키운다.

5. 학습평가방식 Evaluation System

☐ 상대평가(Relative evaluation) ✔ **절대평가(Absolute evaluation)** ☐ 기타(Others): _____

- 평가방식 설명 (explanation of evaluation system):

- 상대평가에 기반한 자율 평가
- 결석 1/3 이상: 학점 F (학칙에 의함)
- 특별한 사유가 아닌 한 재시는 불허

중간고사 Midterm Exam	기말고사 Final Exam	퀴즈 Quizzes	발표 Presentation	프로젝트 Projects	과제물 Assignments	참여도 Participation	기타 Other
40 %	45 %	0 %	0 %	0 %	10 %	5 %	%

Ⅱ. 교재 및 참고문헌 Course Materials and Additional Readings

1. 주교재 Required Materials

Elementary Number Theory (저자: Kenneth H. Rosen, 출판사: Pearson) - 6th edition (Pearson New International Edition)

2. 부교재 Supplementary Materials

3. 참고문헌 Optional Additional Readings

Eementary Number Theory (저자: David M. Burton) 등 기타 수론 관련 학부 전공 서적

Ⅲ. 수업운영 규정 Course Policies

- 수업시간의 3분의 1 이상을 결석한 때는 학칙에 의해 F
- 특별한 사유가 아닌 한 재시는 불허

IV. 참고사항 Special Accommodations

* 학적 제57조에 의거하여 장애 학생은 학기 첫 주에 교과목 담당교수와의 면담을 통해 출석, 강의, 과제 및 시험에 관한 교수학습지원 사항을 요청할 수 있으며 요청된 사항에 대해 담당교수 또는 장애학생지원센터를 통해 지원받을 수 있습니다.

V. 차시별 강의계획 Course Schedule (최소 15주차 강의)

※ 아래의 강의계획안은 수업 진행시 상황에 따라 진도 일정이 변경될 수 있습니다.

주차	날짜	주요 강의내용 및 자료, 과제(Topics & Class Materials, Assignments)
1주차	9월 1일 (수요일)	Introduction to Number Theory
2주차	9월 6일 (월요일)	Well ordering principle, Mathematical induction
	9월 8일 (수요일)	Binomial theorem, Divisibility,
3주차	9월 13일 (월요일)	Integer representation, Computer operations with integers,
	9월 15일 (수요일)	Greatest common divisor
4주차	9월 20일 (월요일)	The Euclidean algorithm, Fundamental Theorem of Arithmetic,
	9월 22일 (수요일)	Prime numbers
5주차	9월 27일 (월요일)	Prime numbers, The distribution of primes
	9월 29일 (수요일)	
6주차	10월 4일 (월요일)	Factorization method and Fermat numbers,
	10월 6일 (수요일)	Linear Diophantine equations, Congruences, Linear congruences
7주차	10월 11일 (월요일)	Chinese remainder theorem, Solving polynomial congruences,
	10월 13일 (수요일)	System of linear congruences
8주차	10월 18일 (월요일)	**정수론 중간고사 일정: 10월 18일(월) 6시–8시30분**
	10월 20일 (수요일)	
9주차	10월 25일 (월요일)	Factoring using Pollard Rho Method, divisibility tests
	10월 27일 (수요일)	
10주차	11월 1일 (월요일)	Wilson's Theorem, Fermat Little Theorem, Pseudoprimes
	11월 3일 (수요일)	
11주차	11월 8일 (월요일)	Euler theorem, Euler phi function, the sum and number of divisors
	11월 10일 (수요일)	
12주차	11월 15일 (월요일)	Perfect numbers and Mersenne primes, Mubius Inversion etc.
	11월 17일 (수요일)	
13주차	11월 22일 (월요일)	Classical and modern cryptography
	11월 24일 (수요일)	
14주차	11월 29일 (월요일)	Public key cryptosystem, Order of an integer and primitive roots
	12월 1일 (수요일)	
15주차	12월 6일 (월요일)	Primitive roots for primes, Discrete log and Index arithmetic etc.
	12월 8일 (수요일)	
16주차	12월 13일 (월요일)	**정수론 기말고사 일정: 12월 14일(월) 6시–8시30분**

VI. 조교

연습 조교	(성명) 김재선 (연구실) 종합과학관 A동 503호 (전화) 3277-3392 (이메일) jaeseon.008@gmail.com