

科目コード／科目名 (Course Code / Course Title)	CA416／情報数理解2演習 (Exercises in Mathematical Information Theory 2)		
担当者名 (Instructor)	安田 雅哉(YASUDA MASAYA) 小山 民雄(KOYAMA TAMIO)		
学期 (Semester)	秋学期(Fall Semester)	単位 (Credit)	1単位(1 Credit)
科目ナンバリング (Course Number)	MAT3410	言語 (Language)	日本語 (Japanese)
備考 (Notes)			

授業の目標(Course Objectives)

「情報数理解1・演習」に引き続き、C言語またはPython言語のプログラミングを通して、やや応用的な数値計算や数理解暗号に関するアルゴリズムとその実装方法について学ぶ。

Following “Mathematical Information Theory 1 and Exercises,” students learn algorithms about somewhat more applicable numerical calculation and mathematical cryptography, and how to implement their algorithms through programming in C or Python language.

授業の内容(Course Contents)

「情報数理解2演習」とペアになる授業である。「情報数理解2」では理論を中心とした講義を行い、「情報数理解2演習」では同一内容のプログラミングからレポート作成までを行う。C言語の文法についてはほぼ習得済みとする。プログラミング作成と数学的理論を利用して、より高度なアルゴリズムの学習やプログラムの作成を行う。内容は、離散フーリエ変換、代数方程式の解法、固有値の計算法、数理解暗号である。「情報数理解2演習」で利用するソフトウェアはC言語が中心になるが、Python言語による数式処理ソフトSageMathも積極的に併用する。

This class is paired with “Exercises in Mathematical Information Theory 2.” “Mathematical Information Theory 2” contains lectures focused on theory, and in “Exercises in Mathematical Information Theory 2” students practice these contents, from programming to report creation. It is assumed that students have just about finished learning the syntax of the C language. Use programming and mathematical theory to learn more sophisticated algorithms and create more advanced programs. Contents include the basics of discrete Fourier Transforms, solving algebraic equations, calculating eigenvalues, and mathematical cryptography. Software used in “Exercises in Mathematical Information Theory 2” centers on the C language, but depending on the problem, other languages or formula manipulation software are used.

授業計画(Course Schedule)

1. 離散フーリエ変換
2. 高速フーリエ変換
3. 高速フーリエ変換の応用
4. 多項式の根: ニュートン法とDKA法
5. 多項式の根: Sturmの方法
6. 固有値の計算法(1): Jacobi法
7. 確認テスト(1)
8. 実対称行列の三重対角化
9. 固有値の計算法(2): べき乗法
10. 楕円曲線暗号と暗号解読(1)
11. 楕円曲線暗号と暗号解読(2)
12. 格子暗号と最短ベクトル問題(1)
13. 格子暗号と最短ベクトル問題(2)
14. 確認テスト(2)

授業時間外(予習・復習等)の学習(Study Required Outside of Class)

授業時間外(予習・復習等)の学習に関する指示は、必要に応じて別途指示する。

成績評価方法・基準(Evaluation)

複数回の課題(12回分)(60%) / 確認テスト(2回分)(40%)
「情報数理解2」と「情報数理解2演習」の単位認定はまとめて行う。

テキスト(Textbooks)

資料を配付する。

参考文献 (Readings)

授業中に紹介する。

その他 (HP 等) (Others (e.g. HP))

注意事項 (Notice)