東京工業高等専門学校	開講年度	平成30年度 (2018年度)	授業科目	情報数学Ⅱ

科目基礎情報

科目番号	0107	科目区分	専門 / 必修
授業形態	授業	単位の種別と単位数	履修単位: 1
開設学科	情報工学科	対象学年	4
開設期	前期	週時間数	2
教科書/教材	植松友彦「代数系と符号理論」オーム社		
担当教員	小嶋 徹也		

到達目標

1. 整数のmod演算を行うことができ，整数における群・環・体の概念を理解する。
2. 多項式環上の加減乗除の計算を行うことができ，これに基づく有限体の概念とその性質を理解する。
3. GF(2)上の原始多項式を用いてM系列を生成する仕組みを理解する。

ルーブリック

	理想的な到達レベルの目安	標準的な到達レベルの目安	最低限の到達レベルの目安（可）	未到達レベルの目安
評価項目1	整数における群・環・体およびその性質を理解し，これらの上で様々な整数演算を実行できる。	整数における群・環・体の概念を理解し，これらの上での整数の加算表や乗算表を作成できる。	教科書などの文献を参照すれば，群・環・体の上で整数の加減乗除算を実行できる。	整数における群・環・体の概念を理解しておらず，これらの上で整数の加減乗除算を実行できない。
評価項目2	多項式がなす環や有限体の概念や性質を理解し，様々な多項式の計算を行うことができる。	多項式がなす環や有限体の概念を理解し，これらの上で多項式どうしの加減乗除算を行うことができる。	教科書やノートなどの資料を参照すれば，環や有限体の上で多項式どうしの計算を行うことができる。	多項式がなす環や有限体の概念を理解しておらず，これらの上での多項式の計算を行うことができない。
評価項目3	GF(2)上の原始多項式を用いてM系列を生成することができ，M系列の性質を理解している。	GF(2)の原始多項式を用いてM系列を生成することができる。	ノートやプリント等の資料を参照すれば，M系列を生成するためのLFSRの動作を説明できる。	GF(2)上の原始多項式を用いてM系列を生成することができない。

学科の到達目標項目との関係

教育方法等

概要	情報数学Ⅰなどで学習したmod演算や集合や写像などに関する内容を踏まえて，整数および多項式を用いた代数系について理解する。また，その応用として，情報通信工学などで利用する乱数系列であるM系列の生成方法を理解する。代数系の上での簡単な計算や，擬似乱数の生成を手計算で行うことができることを主たる目的とする。
授業の進め方・方法	毎回の授業の学習テーマを設定し，その内容について解説する。授業の内容を理解しているかどうか確認するため，毎回簡単な演習問題を課し，提出させる。提出された課題は教員が採点し，原則として次回の授業で返却して解説を行う。定期試験では原則として毎回の課題に類似した内容の問題を出題し，最終的な定着度を確認する。
注意点	mod演算や集合，写像の概念について復習しておくこと。また，毎回授業の最後に演習問題を行う。

授業計画

		週	授業内容	週ごとの到達目標
前期	1stQ	1週	集合の復習	集合の定義や性質を理解する。
		2週	写像の復習	各種写像の定義や性質を理解する。
		3週	整数の除法と最大公約数	負の数を含む整数の除算を行い，商と余りを求めることができ，ユークリッドの互除法を用いて最大公約数および最小公倍数を求めることができる。
		4週	素因数分解と原始根	整数の素因数分解ができ，原始根やオイラーの関数の値を求めることができる。
		5週	群	代数系と群の定義を理解し，代数系上の加算表や乗算表を作成して，その代数系が群であるかどうかを判定できる。
		6週	部分群と同型写像	与えられた部分集合が部分群かどうかを判定することができる。また，群上の写像の像と核を求めることができる。
		7週	巡回群と群の元の位数	群上のべき乗算を行うことができ，群の各元の位数を求めることができる。
		8週	環と体	与えられた代数系が環や体であるか判定できる。
	2ndQ	9週	有限体上の多項式	有限体上で多項式の加減乗除算を行うことができ，最大公約多項式や最小公倍多項式を求めることができる。
		10週	既約多項式	与えられた多項式が既約か可約か判定することができる。
		11週	多項式環	多項式がなす環および有限体について理解し，これらの上で加算表や乗算表を作成することができる。
		12週	原始多項式	与えられた有限体の元が原始根であるかどうかを判定でき，最小多項式および原始多項式を求めることができる。
		13週	有限体の応用～M系列～	LFSRを設計して，M系列を生成することができる。
		14週	M系列の性質と有限体のその他の応用	M系列の性質について理解する。また，有限体を用いて誤り訂正符号などを生成できることを理解する。
		15週	期末試験	
		16週	試験返却，および試験の解説	科目全体を振り返り，各単元について十分に理解し，計算に反映できる。

モデルコアカリキュラムの学習内容と到達目標

分類	分野	学習内容	学習内容の到達目標	到達レベル	授業週

基礎的能力	数学	数学	数学	整式の加減乗除の計算や、式の展開ができる。	3	前9,前10,前11,前12
				行列の定義を理解し、行列の和・差・スカラーとの積、行列の積を求めることができる。	1	前5,前8
				逆行列の定義を理解し、2次の正方行列の逆行列を求めることができる。	1	
				線形変換の定義を理解し、線形変換を表す行列を求めることができる。	1	前5,前8
				平面内の回転に対応する線形変換を表す行列を求めることができる。	1	
専門的能力	分野別の専門工学	情報系分野	計算機工学	基数が異なる数の間で相互に変換できる。	3	
			情報数学・情報理論	集合に関する基本的な概念を理解し、集合演算を実行できる。	4	前1
				集合の間の関係(関数)に関する基本的な概念を説明できる。	4	前2
				ブール代数に関する基本的な概念を説明できる。	4	前5,前6,前7,前9,前10,前11,前12,前13
				離散数学に関する知識をアルゴリズムの設計、解析に利用することができる。	4	

評価割合

	試験	演習問題	合計
総合評価割合	80	20	100
基礎的能力	80	20	100
専門的能力	0	0	0
分野横断的能力	0	0	0