富山高等専門学校	開講年度	平成30年度 (2018年度)	授業科目	応用数学Ⅳ

科目基礎情報

科目番号	0339	科目区分	専門 / 選択
授業形態	授業	単位の種別と単位数	学修単位: 2
開設学科	電子情報工学科	対象学年	5
開設期	後期	週時間数	2
教科書/教材	担当教員の作成した講義資料を毎回配布する		
担当教員	的場 隆一		

到達目標

整数論の概念を用いて情報理論との対応をとりながら講義を行う．素数の性質を理解しながら、それをとりまく定理などを演習を中心として習熟し，RSA暗号の仕組みについて理解する．

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	未到達レベルの目安
評価項目1	ユークリッドの互除法について応用問題や証明問題が解ける．	ユークリッドの互除法について基本問題が解ける．	ユークリッドの互除法について基本問題が解けない．
評価項目2	素数と合同式における応用問題や証明問題が解ける．	素数と合同式における基本問題が解ける．	素数と合同式における基本問題が解けない．
評価項目3	オイラー関数，オイラーの定理，フェルマーの小定理について応用問題や証明問題が解ける．	オイラー関数，オイラーの定理，フェルマーの小定理について基本問題が解ける．	オイラー関数，オイラーの定理，フェルマーの小定理について基本問題が解けない．
評価項目4	公開鍵暗号であるRSA暗号について，その仕組みを詳細に説明でき，暗号化・復号化ができる．	公開鍵暗号であるRSA暗号を用いて暗号化・復号化ができる．	公開鍵暗号であるRSA暗号を用いて暗号化・復号化ができない．

学科の到達目標項目との関係

JABEE B1
ディプロマポリシー 3

教育方法等

概要	担当教員の作成した講義資料を中心に，，各項目について説明を行った後，演習問題を通して理解を深める．
授業の進め方・方法	講義と演習を中心に整数論に関して教授する．講義内容に関する問題について期末試験の点数により評価する．
注意点	評価が60点に満たない者は，本校所定の手続きを経ることで追認試験を受験することができる．追認試験の結果，単位の修得が認められた者にあっては，その評価を60点とする．

授業計画

		週	授業内容	週ごとの到達目標
後期	3rdQ	1週	ガイダンス，演算子の定義 （講義）	自然数とゼロのみの世界に反射率，対象率，推移律を用 いて演算子を定義することに係る内容を理解する．
		2週	法の世界 （講義）	法の概念を理解しする．
		3週	合同式 （講義・演習）	合同式とその性質について理解し，計算できるようになる．
		4週	演習	１週目から３週目までの範囲を振り返り理解度を確かめ ，理解度不足の項目について理解する．
		5週	集合と剰余系 （講義）	集合論の入門知識，および元と写像について理解する．
		6週	フェルマーの小定理１ （講義）	フェルマーの小定理の証明を理解する．
		7週	フェルマーの小定理２ （講義・演習）	フェルマーの小定理の応用について計算できるようになる．
		8週	オイラーの定理１ （講義）	オイラーの定理の証明を理解する．
	4thQ	9週	オイラーの定理２ （講義・演習）	オイラーの定理の応用について計算できるようになる．
		10週	演習	５週目から９週目までの範囲を振り返り理解度を確かめ ，理解度不足の項目について理解する．
		11週	ユークリッドの互除法とエラトステネスの篩 （講義・演習）	ユークリッドの互除法とエラトステネスの篩について理解し，計算できるようになる．
		12週	暗号１ （講義）	公開鍵暗号について理解する．
		13週	暗号２ （講義）	RSA暗号についてその仕組みを理解する．また，素因数分解とその困難性について理解する．
		14週	暗号３ （講義・演習）	RSA暗号により暗号化，復号化できるようになる．
		15週	総合演習	１週目から14週目までの範囲を振り返り理解度を確かめ ，理解度不足の項目について理解する．
		16週	期末試験	整数論および暗号論の知識について出題される試験において，自らの理解度を確認する．

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

評価割合

	試験	発表	相互評価	態度	ポートフォリオ	その他	合計
総合評価割合	100	0	0	0	0	0	100
基礎的能力	100	0	0	0	0	0	100
専門的能力	0	0	0	0	0	0	0
分野横断的能力	0	0	0	0	0	0	0