教科目名　情報数学Ⅰ　(Information Mathematics Ⅰ)

学科名・学年　： 制御情報工学科　5 年　（教育プログラム　第 2 学年　◎科目）
単 位 数 な ど　： 必修　1 単位　（前期 1 コマ，学習保証時間 22.5 時間）
担 当 教 員　： 徳尾健司

授業の概要

公開鍵暗号や誤り訂正符号など，情報科学でよく用いられる事柄の代数学的基礎を与える．前期のⅠでは，初等的な数論 (整数の理論) について，問題演習を交えながら講義する．

達成目標と評価方法　　**大分高専目標(B1)，JABEE 目標(c)(g)**

(1) 剰余の定理とユークリッドの互除法について理解できる．(定期試験と小テスト)
(2) 素数と素因数分解の性質について理解できる．(定期試験と小テスト)
(3) 合同関係と剰余類について理解できる．(定期試験と小テスト)
(4) 1 次合同方程式と中国の剰余定理について理解できる．(定期試験と小テスト)
(5) オイラー・フェルマーの定理について理解できる．(定期試験と小テスト)
(6) RSA 暗号の原理が理解できる．(定期試験と小テスト)

回	授　業　項　目	内　容	理解度の自己点検
1 2 3 4 5 6 7	剰余の定理 最大公約数，最小公倍数，ユークリッドの互除法 1 次不定方程式，連分数 素数，素因数分解 合同，剰余類(1) 剰余類(2)，九去法 復習と応用演習	○ 剰余の定理とユークリッドの互除法について理解する． ○ 素数と素因数分解の性質について理解する． ○ 合同関係と剰余類について理解する． 各内容について，毎回授業の最後に小テストを行い理解度を確認する．	【理解の度合い】
8	前期中間試験		【試験の点数】　　点
9 10 11 12 13 14	前期中間試験の解答と解説，合同式(再) 1 次合同方程式と 1 次不定方程式，中国の剰余定理 オイラーの関数，オイラーの関数の乗法性 フェルマーの定理，位数 原始根，合同方程式の解の個数 平方剰余，公開鍵暗号	○ 1 次合同方程式と中国の剰余定理について理解する． ○ オイラー・フェルマーの定理について理解する． ○ RSA 暗号の原理を理解する． 各内容について，毎回授業の最後に小テストを行い理解度を確認する．	【理解の度合い】
15	前期期末試験		【試験の点数】　　点
	前期期末試験の解答と解説		

履修上の注意	毎回，授業内容の理解を問う小テストを実施するので，授業を良く聞いて理解に努めること．
教　科　書	橘貞雄ほか，「応用代数学入門 ～情報科学へのアプローチ～」，冨山房インターナショナル．
参 考 図 書	小野寛晰，「情報代数」，共立出版． D.W.ハーディほか，「応用代数学入門」，ピアソンエデュケーション．
関 連 科 目	応用数学Ⅰ，Ⅱ，数学演習，情報数学Ⅱ
総 合 評 価	達成目標の(1)～(6)について，2 回の定期試験と毎回授業時の小テストで評価する．総合評価 60 点以上を合格とする． 総合評価 = (定期試験の平均)×0.7 + (小テストの平均)×0.3