

電気通信大学 平成21年度シラバス

授業科目名	現代数学入門B		
英文授業科目名	Introduction to Modern Mathematics B		
開講年度	2009年度	開講年次	1年次
開講学期	後学期	開講コース・課程	昼間コース
授業の方法	講義	単位数	2
科目区分	総合文化科目-理工系教養科目-		
開講学科・専攻	情報通信工学科 情報工学科 電子工学科 量子・物質工学科 知能機械工学科 システム工学科 人間コミュニケーション学科		
担当教官名	大野 真裕		
居室	東1-411		

公開E-Mail	授業関連Webページ
ohno@e-one.uec.ac.jp	なし

<b>【主題および達成目標】</b>
主題：代数学の初歩は，公開鍵暗号のひとつ，RSA暗号などにも使われている．RSA暗号を理解することをめざして，代数学の初歩について学ぶ． 達成目標：RSA暗号の基礎ともなる代数学の初歩を理解すること．

<b>【前もって履修しておくべき科目】</b>
なし

<b>【前もって履修しておくことが望ましい科目】</b>
線形代数学第一，数学演習第一

<b>【教科書等】</b>
教科書：楫元 著「工科系のための初等整数論入門 公開鍵暗号をめざして」（培風館）

【授業内容とその進め方】

(a)授業内容

ユークリッドの互除法

- ・ 整除
- ・ 最大公約数と最小公倍数
- ・ ユークリッドの互除法
- ・ 一次不定方程式

素数

- ・ 素数
- ・ いろいろな素数のタイプ

合同式

- ・ 合同
- ・ 剰余類
- ・ 加減乗
- ・ 除

- ・ 一次合同式

- ・ 連立一次合同式

初等整数論入門

- ・ オイラーの関数
- ・ オイラーの公式
- ・ フェルマーの小定理
- ・ オイラーの定理

公開鍵暗号

- ・ 術語編
- ・ マニュアル編
- ・ 理論編
- ・ 練習編
- ・ 実践編

(b) 授業の進め方

授業は基本的に板書によって進められる。

【授業時間外の学習（予習・復習等）】

論理的に説明されたとしても、新しい概念をすぐにのみこめずに落ちこぼれてしまったり、わかったつもりが勘違いだったりすることは多々ある。しかも、そういった箇所は個人差がある。こういった障害を乗り越えるためにも、土日、連休を利用して、あらかじめ教科書をよんでおくことと強く勧める。こうして準備して講義に臨み、疑問が氷解したとしても、放っておくと、鍵となる視点や考え方を忘れてしまうことがあるので、復習したり、教科書の問題等を実際に解いてみるものが求められる。

## 電気通信大学 平成21年度シラバス

<b>【成績評価方法及び評価基準(最低達成基準を含む)】</b>
剰余類が理解できているか，簡単な一次合同式が解けるか，RSA公開鍵暗号の仕組みが理解できているか，RSA暗号の暗号化と復号化ができるか，という視点から，RSA暗号の基礎が理解できていることを合格の条件とする．  出席状況，レポート提出状況，試験の結果を総合的に加味して評価する．
<b>【オフィスアワー：授業相談】</b>
適宜相談に応じる．
<b>【学生へのメッセージ】</b>
特になし
<b>【その他】</b>
なし