

|      |                                                                                                                 |      |    |                                           |          |      |    |
|------|-----------------------------------------------------------------------------------------------------------------|------|----|-------------------------------------------|----------|------|----|
| 科目名  | 応用数学特論<br>Topics Applied Mathematics                                                                            |      |    | 担当教員                                      | 谷口浩朗     |      |    |
| 学 年  | 1 年                                                                                                             | 学 期  | 前期 | 履修条件                                      | 選択       | 単位数  | 2  |
| 分 野  | 工学基礎                                                                                                            | 授業形式 | 講義 | 科目番号                                      | 11272002 | 単位区別 | 学修 |
| 学習目標 | 有限体および有限体上の平面 3 次曲線について学習する。その応用として暗号や素因数分解への利用を学習する。                                                           |      |    |                                           |          |      |    |
| 進め方  | 準備した教材プリントに基づき、出来るだけ多くの時間を演習に振り向けて、問題を解く手続きの中で、理解を深めながら進む。また適宜課題も与える。                                           |      |    |                                           |          |      |    |
| 学習内容 | 学習項目（時間数）                                                                                                       |      |    | 学習到達目標                                    |          |      |    |
|      | 1. 有限体(8)<br>(1). 有限体<br>(2). 有限体の計算（その 1）<br>(3). ユークリッドの互除法<br>(4). 有限体の計算（その 2）                              |      |    | 有限体に慣れる。 D1:2                             |          |      |    |
|      | 2. 有限体上の平面(2)<br>(1). 有限平面上の直線と曲線の計算                                                                            |      |    | 有限体上の平面に慣れる。 D1:2                         |          |      |    |
|      | 3. 有限平面上の 3 次曲線(8)<br>(1). 有限平面上の 3 次曲線の計算 1<br>(2). 有限平面上の 3 次曲線の計算 2<br>(3). 3 次曲線の群構造<br>(4). 3 次曲線の群構造(乗積表) |      |    | 有限平面上の 3 次曲線の計算が出来るようになる。 D1:1,2          |          |      |    |
|      | 4. 離散対数問題と暗号(6)<br>(1). 離散対数問題と暗号<br>(2). 楕円曲線による暗号<br>(3). デジタル署名                                              |      |    | 離散対数問題を理解する。 D1:1                         |          |      |    |
|      | 5. 素因数分解(6)<br>(1). $\rho$ 法<br>(2). $p-1$ 法<br>(3). 楕円曲線による素因数分解                                               |      |    | いろいろな素因数分解を理解する。 D1:1<br>楕円曲線法を理解する。 D1:1 |          |      |    |
|      | 前期末試験                                                                                                           |      |    |                                           |          |      |    |
|      | 6. 試験問題の解答(1)                                                                                                   |      |    |                                           |          |      |    |
| 評価方法 | 定期試験(70%)，レポート(30%)で総合評価する。                                                                                     |      |    |                                           |          |      |    |
| 履修要件 | 特になし                                                                                                            |      |    |                                           |          |      |    |
| 関連科目 | 基礎数学Ⅱ，応用解析学 → 応用数学特論(1 年)                                                                                       |      |    |                                           |          |      |    |
| 教 材  | 教材プリントを使用 参考書：佐武一郎 著「線型代数学」 数学選書 1 裳華房                                                                          |      |    |                                           |          |      |    |
| 備 考  |                                                                                                                 |      |    |                                           |          |      |    |