

科目名	応用数学特論 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	12272002	単位区別	学修
学習目標	主に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) (1). 有限体 (2). 有限体の計算（その１） (3). ユークリッドの互除法 (4). 有限体の計算（その２）			有限体に慣れる。D1:2			
	2. 離散対数問題と暗号(6) (1). 公開鍵暗号 (2). 離散対数問題と暗号 (3). デジタル署名			公開鍵暗号を理解する。D1:1			
	3. 有限体上の平面(2) (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			
	4. 有限平面上の 3 次曲線(6) (1). 有限平面上の 3 次曲線の計算 1 (2). 3 次曲線の群構造 (3). 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			
	5. 素因数分解(8) (1). ρ 法 (2). $p-1$ 法 (3). 楕円曲線による素因数分解 (4). 楕円曲線による暗号			いろいろな素因数分解を理解する。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						
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	オフィスアワー(月曜 16 時～17 時 30 分)						