地域科学特別演習 I

8 単位 (必修) 1 年 (通年), 2 年 (通年)

片山 真一 · 教授 / 地域科学専攻 (博士前期課程) 基盤科学

【授業目的】代数体の整数論の基礎知識をもとに暗号理論への応用について学ぶ.

【授業概要】代数体での類数，単数について具体的な代数体 (特に 2 次体) での計算 を実行するために連分数展開等のアルゴリズムについて学ぶ．なお代数体の基礎知識を学んだ上で，公開鍵暗号系の基礎について学ぶ．RSA 暗号 ならびに楕円曲線暗号について学び，考察する.

【キーワード】**代数体の整数論，類数，単数，*RSA* 暗号，楕円曲線暗号**

【到達目標】代数体の整数論とその応用の暗号理論について学ぶ.

【授業計画】

1. 1-3 週 (代数体の整数論の基礎)
2. 4-5 週 (類数と単数)
3. 6-8 週 (2 次体での類数と単数)
4. 9-10 週 (連分数展開)
5. 11-13 週 (L 関数)
6. 14-15 週 (類数公式)
7. 16-18 週 (暗号理論の仕組み)
8. 19-20 週 (公開鍵暗号系)
9. 21-23 週 (RSA 暗号)
10. 24-26 週 (楕円曲線)
11. 27-30 週 (楕円曲線暗号)

【成績評価】講義への出席，質疑応答ならびに適宜課する課題レポートによって評価する.

【再試験】原則として再評価はしない

【授業コンテンツ】http://cms.db.tokushima-u.ac.jp/cgi-bin/toURL?EID=218079

【連絡先】

⇒ 片山 (1304, 656-7228, katayama@ias.tokushima-u.ac.jp) Mail (オフィスアワー: 火曜日 15:00-17:00)