応用数理概論 (2)・広域数理科学概論 (4)・応用数理特別講義 II

担当：内田　幸寛

講義の内容

現代の暗号理論では，楕円曲線を用いた暗号が盛んに研究され，実際に利用されている．また，楕円曲線の一般化である超楕円曲線も重要な研究対象である．この講義では，特に有限体上定義されたものを中心に，楕円曲線とその一般化である超楕円曲線について講義する．

具体的な内容は以下の通りである．ただし，状況に応じて変更することがある．

- イントロダクション及びガイダンス
- 楕円曲線の群演算
- 有限体上の楕円曲線
- 楕円曲線暗号
- 超楕円曲線とそのヤコビアン
- 超楕円曲線暗号
- まとめ・レポート

テキスト・参考書等

テキストは特に指定しない．参考書として以下を挙げておく．

- 辻井重男，笠原正雄編著『暗号理論と楕円曲線』森北出版，2008
- N. Koblitz, *Algebraic Aspects of Cryptography*, Springer, 1998（邦訳：林彬訳『暗号の代数理論』丸善出版，2012）
- L. C. Washington, *Elliptic Curves: Number Theory and Cryptography*, 2nd ed., Chapman & Hall/CRC, 2008

成績評価方法

授業参加度 (30%)，レポート (70%) により評価する．

質問受付方法

メール (yuchida@tmu.ac.jp) による質問を随時受け付ける．また，Zoom での質問も受け付けるので，その場合は事前にメールで予約すること．

ウェブページ

http://www.comp.tmu.ac.jp/y-uchida/lectures/2020am2/

講義に関する情報を kibaco とここに掲載する．