

応用数理論 (2) ・ 応用数理論特別講義 II

担当：内田 幸寛

講義の内容

平面上の 3 次曲線として定義される楕円曲線は、現代の整数論において重要な研究対象の一つである。また、楕円曲線は様々な数論アルゴリズムにも利用されており、幅広く応用されている。さらに、楕円曲線の一般化である超楕円曲線についても、楕円曲線と同様の研究手法が利用できることから、様々な研究が進められている。この講義では、楕円曲線とその一般化である超楕円曲線について、それらの応用とともに講義する。

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
- 楕円曲線の応用
- 超楕円曲線とそのヤコビアン
- 超楕円曲線の応用
- 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
- S. D. Galbraith, *Mathematics of Public Key Cryptography*, Cambridge University Press, 2012, <https://www.math.auckland.ac.nz/~sgal018/crypto-book/crypto-book.html>

成績評価方法

授業参加度 (30%), レポート (70%) により評価する。

オフィスアワー

8 号館 6 階 667 室, 火曜 4 時限 (14:40–16:10)

ウェブページ

<https://y-uchida.fpark.tmu.ac.jp/lectures/2024am2/>

講義に関する情報を kibaco とここに掲載する。