2008年度春期

応用数学I[数学科]
応用数学特別講義I[数学専攻]
情報数学特論[理工学専攻情報学領域]

担当：角皆 (つのがい)

1. 授業に関する連絡

主に電子メイル、数学科掲示板 (4 号館 5 階・数学科図書室前)、情報学領域掲示板 (3 号館 2 階・電気電子工学科／情報理工学科事務室前) 及び web page

http://pweb.cc.sophia.ac.jp/tsunogai/kougi/08/ousuu1.html

で行なう。また、角皆への連絡は研究室 (4 号館 5 階 576 室) に直接来てもよいが、電子メイル tsuno@mm.sophia.ac.jp が確実である。

2. 授業の進め方

情報理論・符号理論・暗号理論について、その初歩および基礎となる数学的内容について入門的に紹介する。授業内容の詳細は未定だが、

- 情報理論の入門: 符号化・情報量の理論など
- 符号理論の入門: 誤り訂正符号とその構成など
- 暗号理論の入門: 公開鍵暗号による秘密通信・認証など
- 基礎数理: 有限体とその上の線型代数や Galois 理論・初等整数論など
- 計算量に関する話題: 素因数分解・離散対数問題など

から、受講生の予備知識を鑑みて決める予定。詳しくは上の web page を参照のこと。

3. 評価方法・課題の提出

評価は適宜出題する課題レポートおよび期末試験により行なう予定。レポートは、紙媒体または電子メイルで提出のこと。電子メイルで提出の場合は、**メディアセンターの自分のアカウント**から上記の宛先に提出すること。質問などのメイルも歓迎する。但し、添付ファイルのみのメイルは読まずに消すことがあるので注意。

4. 主な参考書

- 藤原良・神保雅一「符号と暗号の数理」(共立出版)
- J.H. van Lint “Introduction to Coding Theory (3rd ed.)” (Springer-Verlag)
- J.A. Buchmann “Introduction to Cryptography (2nd ed.)” (Springer-Verlag)
- G.A. Jones, J.M. Jones “Information and Coding Theory” (Springer-Verlag)

など。他にも情報理論 (information theory)・符号理論 (coding theory)・暗号理論 (cryptgraphy) などと名の付いた本は多数あるので、適宜参照されたい。基礎数理に関しては、線型代数・有限体・Galois 理論・初等整数論などをキーワードとして探されたい。

— よろづの事どもをたづねて末をみればこそ、事は故あれ。
堤中納言物語「虫愛づる姫君」より