情報セキュリティ特論 (同演習)のページ

【プロローグ】 この講義は有限体上の楕円曲線の理論とその暗号への応用を解説するものです. 主に次の書物の紹介を中心とし, 新しい内容を補ってゆきます.
A. J. Menezes: Elliptic Curve Public Key Cryptosystems.
時間が有れば, 超楕円曲線や, 更に, 関口-三浦の代数曲線暗号についても触れたいと思います.
なお, この講義は恐れ多くも藤原正彦先生の最終年度の院講義と 重なってしまったので, １２限に変更しました.

【実際の講義概要と予定】 講義の進行とともにここに書き込んで行きます.

- ４月１６日(水) : 第１回　楕円曲線と楕円函数の古典論
  この講義で実際に解説するのは有限体上の楕円曲線ですが, 初回は 実数体や複素数体の上の普通の楕円曲線のお話をし, 今後の抽象的理論 を理解しやすくします.
  chap1.pdf本日と次回の講義のノートです.
- ４月２３日(水) : 先週末に引いた風邪がひどくなって突然休講にして しまいました. すみません. １限だと緊急連絡も大変ですね.
- ４月３０日(水) : 第２回　楕円曲線と楕円函数の古典論(続き)
  射影幾何の入門をお話しし, 楕円曲線の群構造の話を完結させた後, 古典論の続きとして, 楕円函数と, 楕円曲線の関係について話しました.
- ５月７日(水) : 第３回　有限体上の楕円曲線
  有限拡大体のお話とその上の幾何学をおさらいし, 有限体上の一般の楕円曲線の基礎事項の説明に入り, 一般の体に対する同型の判定条件を求めた後, 非特異性の条件 と楕円曲線の同型類の指標としての j-不変量の定義までやりました.
  chap2.pdf暗号ショートコースという入門記事 で, 有限素体の復習と, 主に公開鍵暗号に関する常識をおさらいするもの でしたが, 一回休講になったので, このレジュメは最初のところを復習する だけにします. なお, この内容は僕の符号理論 (今年は数理 逍遥 IV と共通で現在進行中) でやったものです.
  chap3.pdfこちらが本日から２～３回の講義のノー トです. (６月２９日 22:15 修正版; Hasse の定理に通し番号を与えたので, 以後の 定理類の番号がずれました. 以後の章の引用の際には御注意ください.)
- ５月１４日(水) : 第４回　楕円曲線の同型類と群構造
  前回の続きです. 楕円曲線の群構造を定義し, 次いでこれと 同型の条件, j-不変量が標数が 2,3 以外のときと 2, 3 のときで どう特殊化されるかを調べます.
- ５月２１日(水) : 第５回　楕円曲線の群構造
  楕円曲線の加法群としての構造に関する定理をいろいろ紹介しました.
  なお, 編集のため chap3.pdf の冒頭に有った有限体の復習を chap2.pdf の方に移し, chap3.pdf に若干の修正を施したので, これらの章の 終了ページが変更になっており, 次の chap4.pdf は 32 ページから 始まります.
- ５月２８日(水) : 第６回　因子
  楕円曲線上の因子の話をしました. イデアルの起源などの雑談が多すぎて, 主因子の定義まで行き着けませんでした.

chap4.pdf本日から２回ほどの講義のノー --トです.(６月２９日 22:23 修正版; Bezout の定理の解説を追加しました.)

- ６月４日(水)：第７回　局所パラメータ
  局所パラメータの定義を与え，局所環の話もちょっと紹介して， 主因子を定義し因子類群を定義しました.
- ６月１１日(水)：第８回　割り算多項式
  楕円曲線の主因子の特徴付けの話を終えた後，割り算多項式の話に入り， その基礎的性質を解説しました.
- ６月１８日(水)：第９回　捻れ群の構造-1
  割り算多項式の性質を用いて，非自明な準同型の全射性の証明まで 行いました.
- ６月２５日(水)：第１０回　捻れ群の構造-2
  次数と準同型の分離性の話をし, 最後に n が体の標数と互いに素な場合の 捻れ群 E[n] の構造定理を証明しました.
- ７月２日(水)：第１１回　Weil ペアリング
  Hasse の定理や Weil の定理の証明のための準備として Weil ペアリング の定義を紹介し, その性質を論じました. chap5.pdf第８回からの話の講義のノート です. まだ３箇所ほど書くつもりで途中になっているところが有りますが, 勉強のために途中でお見せします. あわてて印刷しない方が良いです.
- ７月９日(水)：第１２回　Frobenius 写像
  Weil ペアリングの性質の続きを解説し, Frobenius 写像の話をしました.
- ７月１６日(水)：第１３回　Hasse の不等式・Weil の定理の証明
  今まで準備したことを使ってこれらの基礎的な定理を証明しました. p 冪の捻れ群の構造定理はこれらからすぐ出ますが時間が無くなりました. レジュメを参照してください.
  これで講義の日程は終了しました. 演習の続きをやるかもしれません. 話し終わらなかったことも多いので，後期も多分プライベートなゼミとして 続けます．興味の有る人参加歓迎します.

単位の欲しい人は，レジュメに書いてある問題をいくつか解いて ８月末頃までにレポートとして提出して下さい．専門分野が違うので どうしても解けないと言う人は相談に応じます.
なお, 演習の単位も欲しい人は, がんばってたくさん解いて下さい.

 講義科目の紹介メニューに戻る.