2012年度 第10回の整数論セミナー

日時： 2012 年 6 月 22 日（金） 16:30〜18:00

場所： 〒 169-8555　東京都新宿区大久保 3-4-1
早稲田大学西早稲田キャンパス （旧・大久保キャンパス）
61 号館 4 階 413 室 (61 - 413)

講演者： 志村 真帆呂 （東海大学）

タイトル： 有限体の有限次拡大体上定義された超楕円曲線の被覆曲線の分類と超楕円曲線暗号への応用.（百瀬文之氏，趙晋輝氏との共同研究）

アブストラクト：
超楕円曲線暗号は，有限体上の超楕円曲線の離散対数問題 (DLP) の困難さに依る暗号である．k を有限体，k_d を k の d 次拡大体とする．
k_d 上定義された超楕円曲線 C_0 が k 上定義された被覆曲線 C を持つとき，C_0 のヤコビ多様体 $J(C_0)$ の DLP は $J(C)$ の DLP に帰着できる．
もし，$J(C)$ の DLP が $J(C_0)$ の DLP より計算量が小さければこの攻撃（GHS 攻撃）は成功し，C_0 を weak curve であるという．
本講演では，k 上定義された $(2, 2, ..., 2)$-被覆曲線をもつ k_d 上定義された weak curve の分類と密度についての結果を述べる（主に標数 2 の場合を扱う）．
この結果の一つの応用として，標数 $2, d = 3, C_0$ が楕円曲線の場合，k が素体上の偶数次拡大ならば weak curve の密度は約 $3/4$ となり，奇数次拡大ならば密度が約 $1/2$ となることがわかる．