2013年度 第2回の整数論セミナー

日時： 2013 年 4 月 19 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： 内田 幸寛 （首都大学）

タイトル： Hyperelliptic net による超楕円曲線上の Tate-Lichtenbaum ペアリング

アブストラクト：
代数曲線暗号の理論において，Weil ペアリングや Tate-Lichtenbaum ペアリングのような，代数曲線上のペアリングが重要な役割を果たしている．
近年，Stange は，楕円曲線上の Tate ペアリングを計算する新しいアルゴリズムを提案した．
このアルゴリズムは，Stange によって定義された elliptic net と呼ばれる写像に基づく．
本講演では，elliptic net を超楕円曲線へ拡張して hyperelliptic net と呼ぶべき写像を定義し，その性質を述べる．
また，種数 2 の超楕円曲線上の Tate-Lichtenbaum ペアリングを hyperelliptic net を用いて計算するアルゴリズムを与える．
本研究は内山成憲氏（首都大学東京）との共同研究である．