

第11回情報数理セミナー

日時：2026年9月25日(金)－9月26日(土)

会場：小山工業高等専門学校 講義棟1階 講義室

プログラム

9月25日(金)

8:30－11:00 会場準備・諸注意・自由討論

11:00－12:00 久家 聖二（上智大学）
四次体の類数に関連した一般化 Hurwitz 類数について

12:00－13:30 昼休憩

13:30－14:30 井上 文也（電気通信大学）
秘密分散およびマルチキー準同型暗号を用いたプライバシー保護連合学習について

14:50－15:50 橋本 侑知（東京電機大学）
AGMを用いた同種写像計算とそれらが成すグラフについて

16:10－17:10 佐野 薫（NTT 基礎数学研究センタ）
1量子ビットユニタリ行列の近似限界への Diophantus 近似の応用について

17:10－18:00 自由討論

9月26日(土)

8:30－10:00 会場準備・諸注意・自由討論

10:00－11:00 隈部 哲（東京理科大学）
階乗比の整数性と有限体上の超幾何関数

11:20－12:20 根本 裕介（千葉大学）
The modified diagonal cycles of hypergeometric curves

12:20－13:30 昼休憩

13:30－14:30 臺信 直人（九州大学）
 p -合同な楕円曲線の p -Selmer 群について

14:30－18:00 自由討論

世話人

岡崎 勝男（小山工業高等専門学校 一般科）
金井 和貴（茨城大学大学院 理工学研究科）
神代 真也（大阪工業大学工学部 一般教育科）
品川 和雅（筑波大学 システム情報系）
長峰 孝典（日本大学理工学部 数学科）
宮本 賢伍（茨城大学大学院 理工学研究科）

本セミナーは、以下の助成を受けています。

JSPS 科研費（KAKENHI）若手研究 JP21K13782（研究代表者：品川 和雅）

JSPS 科研費（KAKENHI）若手研究 JP24K16909（研究代表者：神代 真也）

JSPS 科研費（KAKENHI）若手研究 JP24K16885（研究代表者：宮本 賢伍）

JSPS 科研費（KAKENHI）若手研究 JP25K17239（研究代表者：長峰 孝典）

国立高等専門学校機構 研究ネットワーク形成事業（重点支援）（研究代表者：岡崎 勝男）

アブストラクト

久家 聖二（上智大学）

四次体の類数に関連した一般化 Hurwitz 類数について

本講演では、総実代数体上のコーエン・アイゼンシュタイン級数から一般化されたフルヴィッツ類数を定義し、これらを用いて、狭義類数が1の実二次体上の正則ヒルベルトカスプ形式の空間に対するアイヒラー・セルバーグ跡公式を確立する。また、そこから従う類数関係式や密度定理などについて紹介する。古典的なフルヴィッツ類数が虚二次体の類数と結びつくのに対し、本研究で得られるアイヒラー・セルバーグ跡公式に登場する一般化されたフルヴィッツ類数は、四次 CM 体の類数と関係する。本研究は若槻聡氏（金沢大学）および Andrei Seymour-Howell 氏（全南大学）との共同研究である。

井上 文也（電気通信大学）

秘密分散およびマルチキー準同型暗号を用いたプライバシー保護連合学習について

プライバシー保護連合学習（PPFL）とは、参加者間で生データを共有することなく、各クライアントのローカル更新を秘匿したままサーバーに集約し、グローバルモデルを更新する機械学習の枠組みである。その一種として、CCS2019 で Chen らより提案された、CDKS とよばれるマルチキー準同型暗号を応用した PPFL 方式が多数提案されている。CDKS に基づく PPFL では、復号プロセスにおいて、各クライアントが独自の秘密鍵で部分復号した結果をサーバーに安全に伝達する必要がある、この実現方法が課題となっている。本講演ではまず、プライバシー保護の手法として秘密分散と準同型暗号に着目し、提案手法の説明に必要な基礎を解説する。その後、CDKS に基づく PPFL の既存研究を紹介するとともに、秘密分散と CDKS を組み合わせた提案手法について説明する。

橋本 侑知（東京電機大学）

AGM を用いた同種写像計算とそれらが成すグラフについて

代表的な耐量子計算機暗号の1つとして、同種写像暗号がある。同種写像暗号では、頂点を楕円曲線の同型類として、辺をその間の同種写像とするような同種写像グラフと呼ばれるグラフが利用されている。（近年では、種数が2以上の同種写像の成すグラフを利用する方式も多数提案されている。）その同種写像暗号で扱う同種写像グラフとは別のグラフとして、Jellyfish グラフと呼ばれるグラフが知られている。このグラフは arithmetic-geometric mean (AGM) を用いて計算することができて、それが Legendre 曲線間の2-同種写像の計算と対応することが知られている。本発表では、この3-同種写像版を構成し、そのグラフの性質について明らかにした我々の研究成果を発表する。

佐野 薫（NTT 基礎数学研究センタ）

1 量子ビットユニタリ行列の近似限界への Diophantus 近似の応用について

量子計算の分野においては、通常の計算機における $0,1$ の代わりに、複素1次元の単位ベクトルを情報の最小単位として扱う。物理的にはこれは量子の何かしらの状態として実現される。磁場を発生させたり、熱を加えたりする操作により、量子に所望の変化を加えることで、量子ビットの変化を発生させる。したがって連続濃度のパターンの操作が求められるが、物理実装などを想定すると、厳密に実現可能な有限個の操作に絞って、それらを組み合わせることで実現するのが現実的である。つまり、有限個の固定したユニタリ行列の積によって、任意のユニタリ行列を近似する必要がある。Selinger により、この近似を実現する際に用いるユニタリ行列の個数に対する、実現可能な近似精度のオーダーが数値実験により予想されていた。最近、Schmidt の部分空間定理を用いることで、ある程度の広いクラスのユニタリ行列に対してこの予想を解決したので、本講演ではそのことについて解説を行う。本研究は大阪大学の森崎颯太・NTT の秋笛清石との共同研究である。

隈部 哲（東京理科大学）

階乗比の整数性と有限体上の超幾何関数

複素超幾何関数 ${}_nF_{n-1}$ の代数性, およびモノドロミー群の有限性は Beukers–Heckman によって特徴づけられ, そのような超幾何関数を与えるパラメータが分類されている. 一方, 階乗の比のうち常に整数になるものを分類せよという問題は, 古典的な Landau の判定法によってある種の階段関数を分類する問題と結びつき, さらに階段関数が常に 0 または 1 の値をとる場合には, 上記 Beukers–Heckman の分類に帰着させることでその分類が得られることが Rodriguez-Villegas, Bober らによって明らかになっている. 本講演では, これらの分類を有限体上の超幾何関数を用いて捉え直すという講演者による試みを紹介する. 特に, 常に整数となる階乗比を係数とする超幾何関数の有限体類似は整数値をとることを説明する.

根本 裕介（千葉大学）

The modified diagonal cycles of hypergeometric curves

ホモロジー的に自明だが代数的に自明でない代数的サイクルの重要な例として, modified diagonal サイクルがある. しかし, 具体的な曲線に対する modified diagonal サイクルの非自明性を示すことは非常に難しい問題である. 本講演では, 朝倉-大坪によって導入された, Gauss 超幾何関数を複素周期にもつ超幾何曲線を考える. ある仮定のもとで, 超幾何曲線の modified diagonal サイクルの Abel-Jacobi 写像による像が非自明であること示す. 本研究は P. Eskandari 氏との共同研究に基づく.

臺信 直人（九州大学）

p -合同な楕円曲線の p -Selmer 群について

楕円曲線の Selmer 群は, その曲線に付随する様々な数論的不変量の情報を含む重要な対象であり, 多くの観点から研究されている. 素数 p に対し, 二つの楕円曲線 E と A が p -合同であるとは, それらに付随する $\text{mod } p$ Galois 表現 $E[p]$ と $A[p]$ が同型であることをいう. p -合同な二つの楕円曲線の Selmer 群を比較する研究は数多く行われており, 一方の曲線の情報から他方の曲線についての非自明な帰結を導けることから, 様々な応用をもつ. 本講演では, p を奇素数として, 代数体上で定義された楕円曲線 A を固定し, A に p -合同な楕円曲線全体からなる p -合同族を考える. そして, この族に渡る p -Selmer 群の次元を, $A[p]$ 係数の不分岐コホモロジーの次元を基準として捉える新たな視点で考察し, 得られた結果を紹介する. 応用として, p -合同な二つの楕円曲線に対し, それらの p -Selmer 次元の parity の関係を明示的に記述する結果も紹介する. 時間が許せば, 別の応用として, 可視化の理論における Tate–Shafarevich 群の位数 p の元の構成法を, 玉河数の積が p 進単数でない曲線に対して改良できることについても触れる.