第 6 回情報数理セミナー

日時：2024 年 1 月 6 日 (土) ～ 1 月 8 日 (月)
会場: 呉工業高等専門学校 図書館棟 2 階 ラーニングコモンズ

プログラム

1 月 6 日 (土)

9:00～ 会場準備

10:30～12:00 王 贇トウ (大阪大学)
格子解読アルゴリズムの数理構造および解読記録について

13:30～15:00 中村 周平 (茨城大学)
多変数多項式暗号入門

15:30～17:00 橋本 侑知 (東京電機大学)
効率的な CGL ハッシュ関数の構成について

～18:00 自由討論

1 月 7 日 (日)

9:00～ 会場準備

10:30～12:00 任 鑫 (関西大学)
q-deformed rational numbers, q-deformed Farey sum and a special 2-Calabi-Yau category of A_2 quiver

13:30～15:00 後藤 新裕 (九州大学)
Ramanujan–Serre 微分作用素と楕円曲線に関する Kaneko–Sakai の結果について

15:30～17:00 椎井 亮太 (九州大学)
惰性的素数における反円分 $\mathbb{Z}_p$-拡大上の plus/minus Selmer 群の非自明な指数有限 Λ-部分加群について

～18:00 自由討論

1 月 8 日 (月)

9:00～ 会場準備

10:30～12:00 臺信 直人 (慶應大学)
楕円曲線の等分体のイデアル類群の Galois 加群構造について

世話人
金井 和貴 (呉工業高等専門学校 自然科学系分野)
神代 真也 (小山工業高等専門学校 一般科)
品川 和雅 (茨城大学 大学院 理工学研究科)
長峰 孝典 (小山工業高等専門学校 一般科)
宮本 賢伍 (茨城大学 大学院 理工学研究科)

本セミナーは, 独立行政法人国立高等専門学校機構研究ネットワーク形成事業「数学分野と暗号分野の連携ネットワーク」および JSPS 科研費 JP21K13782 の助成を受けています。

アブストラクト

王 贇トウ (大阪大学)

格子解読アルゴリズムの数理構造および解読記録について

Shor の量子アルゴリズムにより、現在利用されている暗号方式は多項式時間で解読できることが数学的に証明されている。量子計算機の開発に伴い、量子計算機に耐性を持つ次世代暗号の研究は必須の課題になっている。暗号方式の安全性解析において、暗号の安全性を代表的な困難問題に帰着し、この問題の効率的な解法が見つかれば、対象とする暗号方式は効率的に破れる。現在、数学の研究対象である格子理論を利用した格子暗号が注目され、格子暗号は次世代暗号の有力な候補になる。格子暗号の安全性は、最短ベクトル問題 (SVP) や近似最短ベクトル問題 (appr-SVP) などの NP 困難性を根拠としている。量子計算モデルにおいても、NP 困難な数学問題は効率的な解読が不可能と期待されている。

本講演では、格子理論の数理基礎をはじめ、(appr-)SVP などの問題解読に用いられる格子簡約アルゴリズムや格子篩法などの数論アルゴリズムを紹介する。そして、最先端の解法となる G6K アルゴリズムを説明し、そのストラテジーを改良したアルゴリズムおよび解読記録について端的に解説する。

中村 周平 (茨城大学)

多変数多項式暗号入門

公開鍵暗号技術は, 攻撃者が秘匿な情報を得る際に困難な数学問題に解くよう設計することで, 情報の取得を困難にする技術である. 現在広く利用されている公開鍵暗号であれば, 素因数分解問題や離散対数問題などの数学問題による困難性が安全性の根拠となっている. しかしながら, これらの数学問題は十分な規模の量子計算機を用いた場合に多項式時間で解けることが 1994 年にショアにより知られており, 近年では大規模な量子計算機の開発に向けた動きが活発化してきている. このような背景から, 量子計算機を用いても解読困難な耐量子計算機暗号を開発することが課題となっており, NIST(米国標準技術研究所) では耐量子計算機暗号の標準化プロジェクトを 2016 年から開始している. 多変数多項式暗号は, この標準化プロジェクトで耐量子計算機暗号の候補として検討されている暗号の一つであり, 現在活発に研究されている暗号である. 本講演では, 多変数多項式暗号の設計及び攻撃の両方について解説することを目指す.

橋本 侑知 (東京電機大学)

効率的な CGL ハッシュ関数の構成について

証明可能安全なハッシュ関数は安全な暗号を構成するための重要な要素技術の 1 つとなっている。その中の 1 つとして CGL ハッシュ関数が提案されている。CGL ハッシュ関数は有限体上の超特異楕円曲線とその間の同種写像の成すグラフ上でのランダムウォークにより構成される。本発表では CGL ハッシュ関数の効率的な構成について解説する。

任 鑫 (関西大学)

q-deformed rational numbers, q-deformed Farey sum and a special 2-Calabi-Yau category of A_2 quiver

Let q be a formal parameter. The left and right q-deformed rational numbers were introduced by Bapat, Becker and Licata via regular continued fractions, and they gave a homological interpretation for left and right q-deformed rational numbers by considering a special 2-Calabi-Yau category associated to the A_2 quiver. In this talk, we begin by introducing these definitions and related results. Then we give a formula for computing the q-deformed Farey sum of the left q-deformed rational numbers based on the negative continued fractions. We combine the homological interpretation of the left and right q-deformed rational numbers and the q-deformed Farey sum, and give a homological interpretation of the q-deformed Farey sum.

後藤 新裕 (九州大学)

Ramanujan–Serre 微分作用素と楕円曲線に関する Kaneko–Sakai の結果について

有理数体 $\mathbb{Q}$ 上の楕円曲線

$$y^2 = x^3 - 1728$$

は $(x, y) = (E_4/\eta^8, E_6/\eta^{12})$ によってパラメータづけすることができる. ここで, E_4, E_6 は Eisenstein 級数, η は Dedekind のエータ関数である. E_4 に Ramanujan–Serre 微分作用素を施したものは E_6 になることからこれを微分方程式とみなすことができる.

Kaneko と Sakai はこのことを一般化し, いくつかの正の整数 N に対し, 合同部分群 $\Gamma_0(N)$(あるいはそのある共役部分群) 上の Eisenstein 級数の満たす微分方程式が $\mathbb{Q}$ 上の楕円曲線を与えることを示した. この操作によって 12 個の楕円曲線が得られるが, これらの楕円曲線に付随する newform という特別な保型形式の族は Ono と Martin による重さ 2 の newform でエータ関数のいくつかの積で書けるような族と完全に一致している. 本講演では, この現象について説明する.

椎井 亮太 (九州大学)

惰性的素数における反円分 $\mathbb{Z}_p$-拡大上の plus/minus Selmer 群の非自明な指数有限 Λ-部分加群について

岩澤理論において, 楕円曲線の Selmer 群が指数有限な Λ-部分加群を持たないことを示すという基本的な問題がある. この問題に関して, R. Greenberg や B. D. Kim などの一連の研究があり, p-部分の Birch Swinnerton-Dyer 予想への応用もある. 本講演では, 研究の背景を説明したあとに, 素数 p が惰性する虚二次体の反円分 $\mathbb{Z}_p$-拡大に対する結果を説明する.

臺信 直人 (慶應大学)

楕円曲線の等分体のイデアル類群の Galois 加群構造について

有理数体 $\mathbb{Q}$ 上の楕円曲線 E と素数 p に対し, E の p 等分体は, $\mathbb{Q}$ に E の p 等分点全てを添加して定まる代数体である. 等分体は円分体の類似物であり, 円分体のイデアル類群に関する Herbrand-Ribet の結果の等分体に対する類似が Prasad や Shekhar らによって研究されている. 講演者は, p で局所的に p 可除な E の有理点を用いて, E の p 等分体 K のイデアル類群を $\mathrm{Gal}(K/\mathbb{Q})$-加群として考察した. 本講演では, この考察の結果得られたイデアル類群のある “既約成分” の重複度の下界に関する結果を紹介する. この結果を応用することで, E の p 等分体のイデアル類群と E の p 進 L 関数の特殊値との間に, ある状況において Herbrand-Ribet の結果に類似した関係が新たに観察できる事にも触れたい.