第 5 回広島整数論集会

アブストラクト

7 月 11 日 (火)

鈴木 正俊 (名大多元)

一次元格子の Epstein ゼータ関数

一次元格子の Epstein ゼータ関数と解釈できるある二変数関数を定義し、それの Chowla-Selberg 公式・Kronecker 極限公式について述べる。またこれの Riemann ゼータ関数の零点分布への応用についても触れたい。

南出 真 (名大多元)・中筋 麻貴 (津田塾大)

セルバーグゼータ関数のアダマール積について

n 次元コンパクトリーマン空間におけるセルバーグゼータ関数は，セルバーグゼータ関数の零点にわたる無限積と，指数が n 次の多項式となる exponential の項との積で表されるアダマール積で表示される．n=3 の場合において，exponential の指数の多項式について，各項の係数を Euler-Selberg constant とラプラシアンの固有値を用いて表示することができたので，その結果を発表する．

宗田 修一 (九大数理)

多重 S 値の特殊値

リーマン・ゼータ関数の 2 以上の整数点での値を一般化したものに多重ゼータ値と多重 S 値というものがあります。多重ゼータ値の特殊値について今までに得られている結果を紹介して、類似のことが多重 S 値についても成立することを述べたいと思います。

7 月 12 日 (水)

河村 尚明 (北大理)

Ikeda lift に付随する Rankin-Selberg 型 Dirichlet 級数について

一般の Siegel cusp 形式に対して、その Fourier-Jacobi 係数の Petersson 内積を用いて定義される Rankin-Selberg 型 Dirichlet 級数は非常に良い解析的性質 (全平面への解析接続, 函数等式) を持つことが知られている。本講演では, 楕円的 Hecke 固有形式 (cusp 形式) の Ikeda lift に付随する Rankin-Selberg 型 Dirichlet 級数の明示公式について述べ、更に, その応用として, Ikeda lift の Petersson 内積が, その 1 番目の Fourier-Jacobi 係数の Petersson 内積と幾つかの L-関数の積を用いて表されることを紹介する。これは, W. Kohnen と N.-P. Skoruppa によって得られた Saito-Kurokawa lift に関する結果の拡張となっている。尚、この結果は、室蘭工業大学の桂田 英典氏との共同研究である。

岡崎 武生 (阪大理)

2 次の Hilbert 保型形式と Siegel 保型形式について

(1) 2 次の Hilbert 保型形式 と同じ L-関数をもつ Siegel 保型形式を構成する方法として吉田リフトがあります。この吉田リフトの non-vanishing problem が L-関数の特殊値と結びつく事や Koecher-Maass 級数が Hilbert 保型形式そのものと関係がある事についてしゃべりたいと思います。

(2)『root number = 1 の Q 上のアーベル曲面に対し、それと同じ L 関数をもつ重さ 2 の Siegel 保型形式が存在する』事が吉田先生により予想されています。しかし、Eichler-Shimura 理論と異なり、重さ 2 の Siegel 保型形式には幾何学的な解釈がされていません。この事などについて、土井-長沼リフトと呼ばれる楕円保型形式から Hilbert 保型形式を構成する方法とからめながら、少ししゃべりたいと思います。

原田 新也 (九大数理)

群の表現の定めるゼータ関数の有理性について (Moon Hyunsuk 氏との共同研究)

G を有限生成な群とし、その有限体 $\mathbb{F}_{q^n}$ 上の d 次表現全部の数を N_n とします。この表現たちは G, d, $\mathbb{F}_q$ で定まる affine scheme の $\mathbb{F}_{q^n}$-有理点の全体と同一視できます。したがって Weil 予想（ゼータ関数の有理性）より、母関数 $Z(G,T) = \exp(\sum_{n=1}^{\infty} \frac{N_n}{n} T^n)$ は T の有理関数になることが分かります。

N_n として、たとえば同型類全体の数をとった場合、この関数がどのような性質をもつのか、またそのことから各 N_n たちの間にある関係性を知ることを期待しています。

これまでの研究で、N_n が絶対既約表現の同型類の個数、N_n が表現の同型類をわたる weighted sum、つまり各 stabilizer の位数の逆数の和の場合について、それぞれ $Z(G,T)$ は T の有理関数、$Z(G,T)$ は $\mathbb{C}$, $\mathbb{C}_p$ 上有理型という結果が得られました。そのことについてお話しします。

森田 知真 (京大理)

p-adic Hodge theory in the imperfect residue field case

K (標数 0) を剰余体 (標数 $p > 0$) が完全な完備離散付値体としたとき、K の絶対 Galois 群の p 進表現についてはかなりのことがわかっている。本講演では K の剰余体が完全でないときの表現について得た結果を紹介し、その応用として Berger の potentially semi-stable theorem の一般化について述べたい。

竹本 隆 (九大数理)

Hilbert symbol と単数群の filtration

局所体上の単数群の filtration に定義域を制限した Hilbert symbol の像の位数に関する結果を紹介します。また、この結果と首都大学東京の川内さんの結果とを組み合わせて、局所体上の楕円曲線の積に対する代数多様体への応用があることも発表します。

星 裕一郎 (京大数理研)

代数曲線の配置空間の基本群のカスプ化について

対数的幾何学を用いた配置空間の基本群の部分的な復元について述べる。また、有限体上の代数曲線の基本群のカスプ化に関する望月新一氏の理論の配置空間への一般化について述べる。

7 月 13 日 (木)

新井 啓介 (東大数理)

４元数体による乗法をもつアーベル曲面に付随するガロア表現の像について

Let $\rho_{E,p} : G_K \longrightarrow \mathrm{Aut}(T_pE) \cong \mathrm{GL}_2(\mathbb{Z}_p)$ be the Galois representation determined by the Galois action on the p-adic Tate module of an elliptic curve E over a number field K. Serre showed that if E has no complex multiplication then $\rho_{E,p}$ has an open image. And I showed that $\rho_{E,p}(G_K)$ has a uniform lower bound for fixed K, p and varying E's. In this talk, I give a similar result on the uniform boundedness of the Galois images associated to abelian surfaces with quaternion multiplication.

原下 秀士 (北大理)

Central streams in the moduli space of abelian varieties

Oort がアーベル多様体のモジュライ空間に foliation という概念を導入した。今回、その一種 (最も重要なものの一つ) である central streams の configuration を決定することができた。この結果等を使うことで、正標数の体上の主偏極アーベル多様体 X が与えられその p-kernel $X[p]$ の群スキームとしての構造が分かっている時、p-divisible group $X[p^\infty]$ の同種類がどれぐらい決定されるかという古典的な問題に対しある意味最良の評価を与えることができる。

川島 学 (名大多元)

多重和のある公式と多重ゼータ値の代数関係式

多重ゼータ値のある新しい関係式族についてお話します。多重和を係数にもつニュートン級数で定義されるある有理型関数 “多重和関数” を考察しますが、多重和のある公式によって “多重和関数” の自然数上でとる値がまた多重和であることが分かります。このことから多重ゼータ値の代数関係式が導かれます。これらの結果と方法についてお話したいと思います。

青木 和麻呂 (NTT 情報流通プラットフォーム)

暗号の中の数学

従来、工学的な応用が考えられなかった整数論も公開鍵暗号の発明以降、暗号分野では様々な利用法が考えられてきた。暗号理論への応用を考える上で、計算量の議論を抜きにすることは出来ず、数学的な考え方と異なる部分も多い。この点さえ許容すれば暗号理論へ利用可能な数学的技術は数多く存在する。本発表では、暗号分野での考え方、暗号理論で求められことを説明し、いくつかの数学的技術の応用例を紹介する。その後、著者が最近手掛けている巨大整数の素因数分解を高速化する上で未解決の問題をいくつか紹介する。

久木宮 到 (中央大理工)

有限体の上の代数曲線 $y^2 = x^7 + a$, $y^4 = x^7 + a$ の有理点の勘定

(仮)

高妻 倫太郎 (九大数理)

Descent theory for elliptic curves related to cyclic cubic extensions

楕円曲線の Mordell-Weil 群と代数体の単数群との間には類似があることが知られている。本講演では代数体の 3 次巡回拡大に付随する代数多様体を導入し、その部分多様体として現れる楕円曲線の基本的性質と降下理論について述べる。

7 月 14 日 (金)

内田 幸寛 (名大多元)

楕円曲線の高さ関数の差の評価

楕円曲線の Mordell-Weil 群や整数点を計算する際、異なる 2 つの高さ関数の差を評価する必要がある。これまでに Zimmer, Silverman, Siksek 等の評価が知られていたが、最近、Cremona-Prickett-Siksek による良い評価が得られた。今回の講演ではその評価の講演者による改良について述べ、いくつかの実例で計算した結果を紹介する。

原本 博史 (広大理)

擬似乱数発生器で、状態をとばすアルゴリズム

擬似乱数とは、$f : S \to S$ を写像とし、S の元 s_0 を初期状態として、漸化式 $s_n := f(s_{n-1})$ により状態を変化させて「乱数のように見える」数列を生成させる手法である。応用上、非常に大きな整数 J に対し、J ステップ後の状態 $f^J(s)$ を計算したいことが良くある（ジャンプ）。

S が二元体上の d 次元空間 $(\mathbb{F}_2)^d$ であり、f が線形写像であるものが広く用いられている。メルセンヌツイスター法はその一例であり、$d = 19937$ である。f の行列表示を用いると、19937 次正方行列の積を計算することになり、効率が悪い。J 乗を計算すること自体が困難である。

ここでは、$g(t) := t^J \bmod (f \text{ の最小多項式})$ をあらかじめ計算しておき、$g(f)s$ を計算することによる高速なジャンプの手法を導入する。

この計算で特徴的なのは、f として高速計算可能な漸化式を選んでいるため、$s \to f(s)$ の計算のほうが、$s_1, s_2 \to s_1 + s_2$ の計算より 100 倍程度高速であるということである。

このため、この計算問題は「多項式 $g(f)$ を計算するのに、どうすれば足し算の個数を　少なくできるか（掛け算はあまり負担にならない）」という問題に帰着される。

我々は $g(f)s$ を計算するため、あらかじめ次数の低い多項式 h_i に対して、$h_i(f)s$ を計算し表にしておく作戦をとった。このとき計算時間とメモリ使用量に関して、結果を発表する。

この研究は松本眞氏、Pierre L'Ecuyer 氏、西村拓士氏、Francois Panneton 氏との共同研究である。