様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

# 科学研究費助成事業　　研究成果報告書

平成　２９　年　　６　月　１６　日現在

機関番号：　１８００１
研究種目：　若手研究(B)
研究期間：　2014～2016
課題番号：　２６８０００２０

研究課題名（和文）跡公式を用いた素測地線分布とスペクトル分布に関する研究

研究課題名（英文）Research on distributions of prime geodesics and spectra of Laplacians on hyperbolic manifolds

研究代表者

橋本　康史（HASHIMOTO, Yasufumi）

琉球大学・理学部・准教授

研究者番号：３０４５２７３３

交付決定額（研究期間全体）：（直接経費）　　3,000,000円

研究成果の概要（和文）：実階数1の半単純リー群の離散部分群によって与えられる体積有限な双曲多様体において，素測地線の分布とラプラシアンのスペクトルの分布との間には密接な関係があり，各々が多様体（の基本群）を特徴づける重要な要素である．本研究ではこれらの２つの分布をセルバーグの跡公式を用いて関連付けながら調べることで，多様体を特徴づけることを目的としている．本研究期間中には、素測地線定理に付随する極限公式を用いて合同部分群に関するセルバーグゼータ関数の非絶対収束域における値の評価を行った．加えて，ヘッケ作用素に関する跡公式と強い関連性のある２次形式の類数和に関する漸近評価を導いた．

研究成果の概要（英文）：It has been well-known that there are deep connections between the distributions of primitive geodesics and spectrum of the Laplacian for hyperbolic manifolds derived from discrete subgroups of semi-simple Lie group, and they are important factors to characterize manifolds (and their fundamental groups). In this research, we aim to study these distributions by using Selberg's trace formula. We proposed, in this research, estimations of the values of Selberg's zeta functions for congruence subgroups on the non- absolute convergence areas by using a limit formula derived from the prime geodesic theorem. We further obtained an asymptotic formula for class number sums of quadratic forms associated with the trace formulas for Hecke operators.

研究分野：　数物系科学

キーワード：　跡公式　セルバーグゼータ関数　length spectrum　ラプラシアン　不定値2元2次形式

## １．研究開始当初の背景

実階数１の半単純リー群の離散部分群によって与えられる体積有限な双曲多様体において，素測地線の分布とラプラシアンのスペクトルの分布との間には密接な関係があり，各々が多様体（の基本群）を特徴づける重要な要素である．とくに，多様体（またはその基本群）の数論性・非数論性（arithmeticity, non-arithmeticity）に関しては，ラプラシアンの例外固有値の存在・非存在性，非コンパクト多様体に関する cuspidality，スペクトルのばらつきをあらわす number variance とよばれる関数の挙動，length spectrum およびその重複度の分布，など，いずれも完全に解決されていないが，素測地線の分布やスペクトルの分布との関連性を示唆する（数値実験を含む）研究成果が主に 1980 年代以降得られている．セルバーグの跡公式は，これらの分布の間の関連性をあらわす公式のひとつであるが，解析数論における，素数とリーマンゼータ関数の非自明零点の間の関係をあらわすヴェイユの明示公式や，数理物理における，古典系の周期軌道と量子化した系の固有エネルギーとの間の関係を表わすグッツヴィラーの跡公式に酷似していることから，本研究で用いられる手法や成果は，整数論や数理物理の研究においても重要な役割を果たすと期待できる．

## ２．研究の目的

一般的なリーマン多様体において，同じ長さをもつ素測地線はほとんどない（length spectrumの重複度はほとんど1である）ことが多いことが知られているが，体積有限な双曲平面上では重複度が常に非有界であることが Randol (1980）によって示されている．とくに，数論的（arithmetic）な多様体については重複度が高くなる傾向がある．実際に Bogomolny-Leyvraz-Schmit (1996), Peter (2002)，Lukianov (2007)，本研究代表者 (2013）らの研究によって，モジュラー群の合同部分群を基本群にもつ非コンパクトな数論的双曲平面に関するlength spectrumの重複度のべき和に関する漸近公式が得られており，それらの結果は，数論的多様体に関する length spectrum が高い重複度をもつことを示唆している．本研究では，これらの成果をより一般的な数論的多様体に拡張するとともに，このような重複度に関する研究成果を，セルバーグの跡公式に適用することで，セルバーグゼータ関数の特殊値の評価や，ラプラシアンの固有値の漸近的な挙動・最小固有値の評価へと応用し，より多角的に多様体の特徴づけをおこなうことを目標とする．

## ３．研究の方法

多様体の特徴づけを行う際，素測地線の長さの集合であるlength spectrum が，ラプラシアンのスペクトルと同程度の情報をもっていることはよく知られているが，length spectrum をわかりやすい形で記述することは一般的には非常に難しい．ただ，基本群がモジュラー群やモジュラー群の合同部分群である場合には length spectrum は２次形式の基本単数と類数を用いて表されている．このような「よりわかりやすい」length spectrumの表示をより一般的な基本群で導くことで，素測地線分布に関する情報が得られることが期待できる．さらに，セルバーグの跡公式に素測地線分布に関する研究成果を適用することで，ラプラシアンのスペクトルの分布に関する情報が得られると考えられる．

## ４．研究成果

(1) 合同部分群に関するセルバーグゼータ関数の値の評価

モジュラー群に関するセルバーグゼータ関数の絶対収束域での値が不定値2元2次形式の基本単数と類数を用いて記述できることは，1980年代には示されている．モジュラー群の合同部分群に対しても同様に，length spectrum の重複度が類数を用いて表されることから，モジュラー群の場合と同様の表示が得られている．このことから，古典的に知られていた類数の評価を用いて，合同部分群に関するセルバーグゼータ関数の絶対収束域での値を評価することができる．一方で，非絶対収束域については，セルバーグの跡公式を用いた解析接続が知られているが，その解析接続の公式を直接用いて値を評価するのは必ずしも簡単ではない．本研究では，非絶対収束域におけるセルバーグゼータ関数を，素測地線定理に付随する極限公式を用いてあらわし，その表示に類数公式や素測地線定理の誤差項評価を行う際に使われた手法を適用することで，ラプラシアンの例外固有値から得られる特異点を除く実軸上の点において，セルバーグゼータ関数の値の評価を行うことができた．さらに，モジュラー群については，指数和に関する van der Corput の手法を適用することで，さらに実軸上を除く点についても値の評価を従来のものよりも改良することができた．

(2) ペル型の方程式が可解な判別式に関する不定値2元2次形式の類数和の漸近公式

この研究成果は，直接的には研究テーマに即しているわけではないが，モジュラー群や合同部分群に関する length spectrum や素測地線定理との関連性が深い．2元2次形式の類数は，『ガウス整数論』にも言及されているように長い歴史を持つ研究対象であり，類数1問題や Cohen-Lenstra's heuristic など未解決問題も少なくなく，その分布を調べることは整数論において重要な課題のひとつである．その中で，Gauss によって予想され Siegel によって証明された「判別式の小さい順に」類数和をとったものに関する漸近公式は，現在では概均質ベクトル空間の研究に発展している一方，Sarnakによって証明された「基本単数の順に」類数和をとったものに関する漸近公式は，モジュラー群に関する素測地線定理から導かれたものであり，跡公式やセルバーグゼータ関数の研究と強い関連性をもっている．本研究成果は，Sarnak型の漸近公式を，すべての判別式ではなく，「ペル型の方程式が解をもつ」ような判別式に関する類数和に定式化し，漸近公式の主要項が明示的な形で導いた．このような漸近公式は，すべての判別式で和をとったものとの比較を行うことで，ペル型の方程式の可解性の観点から，整数論的にも興味深いと考える．さらに，このような漸近公式は，ヘッケ作用素に関する跡公式と深い関連性をもつため，length spectrum やラプラシアンのスペクトル分布を調べる際にも有用であると期待できる．

５．主な発表論文等

（研究代表者，研究分担者及び連携研究者には下線）

(*)は査読付

〔雑誌論文〕（計　8 件）


1.(*) C.M. Cheng, Y. Hashimoto, H. Miura and T. Takagi, A polynomial-time algorithm for solving a class of underdetermined multivariate quadratic equations over fields of odd characteristics, Springer LNCS, Vol. 8772, pp.40-58, 2014.

2. (*) Y. Hashimoto, Cryptanalysis of the multivariate signature scheme proposed in PQCrypto 2013, Springer LNCS, Vol.8772, pp.108-125, 2014.

3. (*) H. Miura, Y. Hashimoto, T. Takagi, Extended algorithm for solving under-defined multivariate quadratic equations, IEICE Trans. Fundamentals, Vol. 97-A, pp.1418-1425, 2014.

4. (*) Y. Hashimoto, Cryptanalysis of the quaternion Rainbow, IEICE Trans. Fundamentals, Vol. 98-A, pp.144--152, 2015.

5. (*) Y. Hashimoto, Cryptanalysis of the multivariate signature scheme proposed in PQCrypto 2013, IEICE Trans. Fundamentals, Vol. 99-A, pp.58-65, 2016.

6. 橋本康史, 合同部分群に関する length spectrum の重複度について, 数理解析研究所講究録, Vol. 2013, pp.100-109, 2016.

7. (*) Y. Hashimoto, Key recovery attacks on multivariate public key cryptosystems derived from quadratic forms over an extension field, IEICE Trans. Fundamentals, Vol. 100-A, pp.18-25, 2017.

8. (*) Y. Hashimoto, Chosen ciphertext attack on ZHFE, JSIAM Letters, Vol. 9, pp.21-24, 2017.


〔学会発表〕（計　18 件）


1. 橋本康史, ペル型方程式が可解な判別式に関する類数和の漸近的な挙動について, 2014 年度日本数学会代数学分科会, 学習院大学（東京都豊島区）, 2014 年 3 月 18 日.

2. 橋本康史, Pell 型の方程式 t^2-Du^2=4N が可解な判別式に関する類数和について, 研究集会「2014 表現論がつなぐ数学」, サンポートホール高松（香川県高松市）, 2014 年 9 月 29 日.

3. (*) C.M. Cheng, Y. Hashimoto, H. Miura and T. Takagi, A polynomial-time algorithm for solving a class of under-determined multivariate quadratic equations over fields of odd characteristics, Sixth International Conference on Post-Quantum Cryptography, University of Waterloo (Waterloo, Canada), 2014 年 10 月 2 日.

4. (*) Y. Hashimoto, Cryptanalysis of the multivariate signature scheme proposed in PQCrypto 2013, Sixth International Conference on Post-Quantum Crypto -graphy, University of Waterloo (Waterloo, Canada), 2014 年 10 月 3 日.

5. Y. Hashimoto, On the values of Selberg's zeta functions for congruence subgroups, Zeta Functions in OKINAWA 2014, 沖縄コンベンションセンター（沖縄県宜野湾市）,

2014 年 10 月 27 日.
6. 橋本康史, 合同部分群に関する length spectrum の重複度について, RIMS 研究集会「解析的整数論 — 数論的対象の分布と近似」, 京都大学数理解析研究所（京都府京都市）, 2014 年 10 月 30 日.
7. 橋本康史, 素因子の上位ビットが既知で秘密鍵が小さい RSA に対する攻撃法について, 首都大整数論セミナー, 首都大東京（東京都八王子市）, 2014 年 11 月 14 日.
8. 橋本康史, 拡大体型の多変数連立2次方程式暗号の安全性について, 研究集会「表現論がつなぐ数学 2015」, JR 九州ホテル鹿児島（鹿児島県鹿児島市）, 2015 年 9 月 17 日.
9. 橋本康史, 多変数版 HFE の安全性について, 2015 年度日本応用数理学会年会, 金沢大学（石川県金沢市）, 2015 年 9 月 11 日.
10. 橋本康史, Estimations of Selberg's zeta functions for congruence subgroups, Zeta Functions in OKINAWA 2015, 沖縄コンベンションセンター（沖縄県宜野湾市）, 2015 年 10 月 10 日.
11. 橋本康史, 多変数多項式暗号, Crest 暗号数理チュートリアルワークショップ, 九州大学（福岡県福岡市）, 2015 年 12 月 15 日.
12. 橋本康史, 多層な Rainbow の安全性について, 2016 年度暗号と情報セキュリティシンポジウム, ANA クラウンプラザホテル熊本ニュースカイ（熊本県熊本市）, 2016 年 1 月 20 日.
13. Y. Hashimoto, On the security of ZHFE, Fukuoka Workshop on Multivariate Cryptography, 九州大学, 2016 年 3 月 25 日.
14. 橋本康史, 合同部分群に関するセルバーグゼータ関数の値の評価, 研究集会「表現論がつなぐ数学 2016」, 沖縄県男女共同参画センター「てぃるる」（沖縄県那覇市）, 2016 年 9 月 9 日.
15. 橋本康史, ZHFE に対する選択暗号文攻撃, 2016 年度日本応用数理学会年会, 北九州国際会議場（福岡県北九州市）, 2016 年 9 月 12 日.
16. Y. Hashimoto, On values of Selberg's zeta functions for the modular group, Zeta Functions in OKINAWA 2016, 沖縄コンベンションセンター（沖縄県宜野湾市）, 2016 年 10 月 29 日.
17. 橋本康史, 多変数多項式暗号の暗号化速度の改良, 2017 年度暗号と情報セキュリティシンポジウム, ロワジールホテル那覇（沖縄県那覇市）, 2017 年 1 月 26 日.
18. **[特別講演]** 橋本康史, 合同部分群に関する length spectrum の重複度の分布について, 2017 年度日本数学会年会函数解析学分科会, 首都大学東京（東京都八王子市）, 2017 年 3 月 26 日.

〔図書〕（計　0 件）

〔産業財産権〕

○出願状況（計　0 件）

名称：
発明者：
権利者：
種類：
番号：
出願年月日：
国内外の別：

○取得状況（計　0 件）

名称：
発明者：
権利者：
種類：
番号：
取得年月日：
国内外の別：

〔その他〕
なし

## ６．研究組織

(1)研究代表者
橋本　康史（HASHIMOTO, Yasufumi）
琉球大学理学部数理科学科・准教授
研究者番号：30452733

(2)研究分担者
なし

(3)連携研究者
なし

(4)研究協力者
なし