様式 C-19

科学研究費補助金研究成果報告書

平成２３年６月２０日現在

機関番号：87103
研究種目：若手研究（B）
研究期間：平成２０年度～平成２２年度
課題番号：20740027
研究課題名（和文）　ゼータ関数と跡公式による密度分布定理と不変量に関する研究
研究課題名（英文）　Research on density theorems and invariants with zeta functions and trace formulas

研究代表者
橋本 康史（Yasufumi Hashimoto）
財団法人九州先端科学技術研究所・情報セキュリティ研究室・研究員
研究者番号：30452733

研究成果の概要（和文）：
リーマンゼータ関数と素数定理、セルバーグゼータ関数と素測地線定理に代表されるように、ゼータ関数と密度分布定理の間には密接な関係がある。本研究では、ゼータ関数や跡公式を用いて、密度分布やそれに付随する不変量に関する研究を行うことで、空間や多様体の性質を明らかにすることを目的とする。とくに、双曲多様体上の閉測地線の長さの集合として定義される length spectrum は多様体の特徴付けにおいて重要であり、研究期間中に数論的な多様体に関する length spectrum を数論的な対象を用いて明示的に記述すること、そして、その記述を用いて length spectrum の重複度の「平均的な」分布を表わす漸近公式を導くことができた。さらに、副産物として、不定値 2 元 2 次形式の類数の分布のある種の精密化を行うことができた。

研究成果の概要（英文）：
There are deep connections between zeta functions and density theorems, such like Riemann's zeta functions and the prime number theorem, Selberg's zeta functions and the prime geodesic theorem. In this research, we aim to explain the properties of manifolds by studying density theorems and invariants with zeta functions and trace formulas. Especially, the length spectrum defined by the set of length of closed geodesics on a hyperbolic manifold is important to characterize the manifold. The main results on this research is to describe the length spectra for arithmetic surfaces in terms of objects in the classical number theory, and to obtain an asymptotic formula to explain ``average" of the behavior of the multiplicity of the length spectrum. As an application, we also get one kind of improvements of the asymptotic formula for the class numbers of indefinite binary quadratic forms.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
平成 20 年度	1,100,000	330,000	1,430,000
平成 21 年度	900,000	270,000	1,170,000
平成 22 年度	900,000	270,000	1,170,000
総　計	2,900,000	870,000	3,770,000

研究分野：数物系科学
科研費の分科・細目：数学・代数学
キーワード：ゼータ関数、 跡公式、素測地線定理、length spectrum、ラプラシアン

１．研究開始当初の背景

本研究で取り扱った、体積有限な双曲多様体上の素な閉測地線の個数に関する漸近公式である素測地線定理と、素数の個数に関する漸近公式である素数定理の間には、その誤差項がそれぞれに対応するゼータ関数の非自明零点によって与えられる、といった類似性がある。このため、研究対象自体は、微分幾何的なものであるものの、解析数論的にも重要なものであると考えられている。加えて、素測地線定理やセルバーグゼータ関数の性質を調べる際に用いられるセルバーグ跡公式が、量子カオスにおけるグッツヴィラーの跡公式に類似していることから、閉測地線の分布や（セルバーグゼータ関数の非自明零点を与える）ラプラシアンの固有値の分布は、数理物理においても、重要な研究対象であるといえる。

２．研究の目的

素測地線定理と素数定理の分布に関しては、前述したような類似性があるものの、相違点として、素測地線定理に関しては、同じ長さをもつ測地線がたくさんあることが挙げられる。この長さの重複の様子は、それぞれの多様体によっても異なっていると考えられており、とくに、多様体の（基本群の）数論性（arithmeticity）によって特徴づけられるであろうことが、先行研究における数値実験や部分的な結果の証明によって、指摘されている。一方で、ラプラシアンの固有値についても、その分布がリーマンゼータ関数の非自明零点の分布と異なっており、分布のばらつきの様子が、多様体、とくにその数論性と関連性があることが指摘されている。本研究では、このような、測地線とラプラシアンの固有値の分布の様子を明らかにすることで、多様体の特徴付けを行うことを目的とする。

３．研究の方法

素測地線に関して、長さの情報は、多様体の特徴づけという観点から重要な情報を含んでいる。実際に、素測地線の長さの集合である length spectrum を重複度込みで決定することと、ラプラシアンの固有値を決定することが同値であることは、1960 年ごろにはすでに証明されている。しかしながら、length spectrum は初等的に記述できる対象ではなく、lenth spectrum を「よりわかりやすい」対象を用いて記述することは、必要不可欠である。本研究では、この観点から、合同部分群に関する length spectrum を、古典数論的な研究対象である、2 次形式の類数によって明示的に記述することと、その記述を用いて、重複度の分布を調べることに取り組んだ。

４．研究成果

(1) モジュラー群の合同部分群に関するセルバーグゼータ関数の数論的な表示.

モジュラー群に関するセルバーグゼータ関数が不定値 2 元 2 次形式の基本単数と類数を使って記述できることは 1980 年代に Sarnak によって示されており、また、代表的な合同部分群である $\Gamma_0(N), \Gamma_1(N), \Gamma(N)$ に対しては、2007 年に本研究代表者によって、同様に記述できることが示されている。この表示式は、一般にはその性質がよくわからない length spectrum を、類数という古典的な研究対象を用いて記述している、という点で、有用であると考える。本研究では、モジュラー群によって定まるリーマン面上の測地線が、合同部分群によって定まるリーマン面上で分解する様子が、2 次形式の判別式の算術的な性質を用いて記述できることを利用して、セルバーグゼータ関数を「すべての」合同部分群に対して、2 次形式の類数と基本単数を用いて記述することができた。

(2) 合同部分群に関する length spectrum の重複度の分布.

一般的に、length spectrum の分布を調べることは簡単ではない。しかしながら、モジュラー群に関しては、Bogomolny-Leyvraz-Schmit (1996) と Peter (2002) によって、length spectrum の重複度の 2 乗和の増大度を表す漸近式が得られている。本研究では、(1)の成果を利用して、モジュラー群の「任意の」合同部分群に対して、重複度の「任意の」冪和に関する漸近公式を導いた。漸近式の主要項の係数は、ある有限群上の算術的な性質をみたす共役類の割合を使って記述できており、与えられた合同部分群に対して、その係数の具体的な値を計算することが容易である。この値によって、重複度の分布のばらつき、一様性の様子の解析ができることが期待できる。

(3) 不定値 2 元 2 次形式の類数和に関する漸近公式.

(1)(2)の研究の副産物として、2 次形式の類数に関する研究成果を得た。不定値 2 元 2 次形式の類数は、数百年の歴史をもつ研究対象であり、類数 1 問題や Cohen-Lenstra の Heuristic などの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といえる。Gauss によって、「判別式の順に」類数の和をとったものに関する漸近公式が予想されており、1940 年代に Siegel によって証明が与えられた。この Siegel による成果は、現在では、慨均質ベクトル空間のゼータ関数の研究へと展開している。これに対して、1980 年代に Sarnak は「基本単数の順に」類数の和をとっ

たものに関する漸近公式を導いた。これは、モジュラー群に関する素測地線定理を、2 次形式と素測地線との対応を用いて記述しなおしたものであり、幾何的なアプローチであるといえる。本研究では、この Sarnak 型の類数和の漸近公式を、判別式に関する算術的な条件によって細分化した。(1)の研究から、判別式の算術的な条件と、モジュラー群と主合同部分群から与えられる有限群の共役類に関する算術的な条件が対応することが分かっているので、Tchebotarev 型の素測地線定理をいくつか組み合わせることで、類数和に関する漸近公式の細分化を導くことができる。実は、同様の研究はすでに Raulf によって行われていたが、漸近公式の主要項の係数の表示の分かりやすさ、誤差項の評価、アプローチの汎用性の高さという点で、本研究の成果は優れていると考えられる。

(4) 今後の課題.

本研究では、おもに、モジュラー群の合同部分群を基本群として持つ 2 次元の双曲多様体上の length spectrum に関する成果が得られた。この研究成果を、合同部分群以外の基本群、・3 次元以上の多様体、に対して拡張することが、今後の課題である。また、Rudnick によって示されたように、length spectrum の重複度の冪和に関する漸近式の主要項の係数が、ラプラシアンのスペクトルのばらつきを表す公式にあらわれることから、本研究の成果をラプラシアンのスペクトルの分布の研究に応用することも、今後の課題の一つである。

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）

〔雑誌論文〕（計 7 件）(すべて査読有)

1. Y. Hashimoto, *Analytic properties of partial zeta functions*, RIMS Kokyuroku Bessatsu B-7, pp.73-82, 2008.

2. Y. Hashimoto, *Distributions of multiplicities in length spectra for hyperbolic Riemann surfaces*, OCAMI Studies 2-2, pp.195-199, 2008.

3. Y. Hashimoto, *Prime and zero distributions for meromorphic Euler products*, 5th Asian Mathematical Conference Proceedings 1, pp.255 - 261, 2009.

4. Y. Hashimoto, *On asymptotic behavior of composite integers n=pq*, J. Math-for-Industry 1, pp.45-49, 2009.

5. Y. Hashimoto, *Algorithms to solve massively under-defined systems of multivariate quadratic equations*, Proceedings (Industrial Track) of the 8th International Conference on Applied Cryptography and Network Security, pp.26–37, 2010.

6. Y. Hashimoto, *On small secret key attack against RSA with high bits known prime factors*, Proceedings (short papers) of 5th International Workshop on Security, pp.14–25, 2010.

7. Y. Hashimoto, *Partial zeta functions*, Archiv der Mathematik 95, pp.363–372, 2010.

〔学会発表〕（計 19 件）（*は査読有）

1. 橋本康史, 不定値二元二次形式の類数の部分和に関する漸近公式について, 2008 年度日本数学会年会代数学分科会, 東京工業大学, 2008 年9 月.

2. 橋本康史, $n = pq$ 型の合成数の分布について, Zetas and Limit Laws in OKINAWA 2008, 沖縄コンベンションセンター（沖縄県宜野湾市）, 2008 年11 月.

3. 橋本康史, 変数の個数が方程式の個数よりも十分大きい多変数連立二次方程式の解法について, 2009 年度暗号と情報セキュリティシンポジウム, 大津プリンスホテル（滋賀県大津市）, 2009 年1月.

4. 橋本康史, 変数の個数が方程式の個数よりも十分大きい多変数連立二次方程式の解法について, ワークショップ「安全な社会基盤への計算量的数論の応用–次世代暗号技術の最先端理論より–」, 九州大学, 2009 年3 月.

5. Y. Hashimoto, *Prime and zero distributions for meromorphic Euler products*, 5th Asian Mathematical Conference, Putra World Trade Centre （マレーシア, クアラルンプール市）, 2009 年6 月.

6. 橋本康史, オイラー積で表される有理型なゼータ関数の素元分布と零点分布について, 研究集会「表現論がつなぐ数学」, ホテルロコアナハ（沖縄県那覇市）, 2009 年9 月.

7. Y. Hashimoto, *Asymptotic formulas of*

class number sums in arithmetic progressions for indefinite binary quadratic forms, Zetas and Limit Laws in OKINAWA 2009, フェストーネ（沖縄県宜野湾市）, 2009 年11 月.

8. 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, 2010 年度暗号と情報セキュリティシンポジウム, サンポートホール高松（香川県高松市）, 2010 年1 月.

9. 橋本康史, 不定値二元二次形式の類数和に関する漸近公式について, 第15 回代数学若手研究会, 名古屋大学, 2010 年3 月.

10. 橋本康史, 不定値二元二次形式の類数和に関する漸近公式について, 2010 年度日本数学会年会代数学分科会, 慶応義塾大学, 2010 年3 月.

11. Y. Hashimoto, *Algorithms to solve massively under-defined systems of multivariate quadratic equations*, Industrial Track in 8th International Conference on Applied Cryptography and Network Security, 北京工大建国飯店（中国北京市）, 2010 年6 月.

12. 橋本康史, 不定値二元二次形式の類数和に関する漸近公式, 第9 回仙台広島整数論集会, 東北大学, 2010年7 月.

13. 橋本康史, 不定値二元二次形式の類数和に関する漸近公式, 大阪大学整数論・保型形式セミナー, 大阪大学, 2010 年7 月.

14. 橋本康史, 不定値二元二次形式の類数和に関する漸近公式, 研究集会「表現論がつなぐ数論・解析学・組合せ論」, 愛媛大学, 2010 年8 月.

15. 橋本康史, 合同部分群に関する*length spectrum* の重複度について, 2010 年度表現論シンポジウム, おおとり荘（静岡県伊豆の国市）, 2010 年11 月.

16. Y. Hashimoto, *On multiplicities in length spectra for congruence subgroups*, Zetas and Limit Laws in OKINAWA 2010, 沖縄コンベンションセンター（沖縄県宜野湾市）, 2010 年11 月.

17. Y. Hashimoto, *On small secret key attack against RSA with high bits known prime factors*, 5th International Workshop on Security (IWSEC2010), 神戸国際会議場（兵庫県神戸市）, 2010 年11月.

18. 橋本康史, 高木剛, 多変数暗号に関する故障利用攻撃について, 2011 年度暗号と情報セキュリティシンポジウム, リーガロイヤルホテル小倉（福岡県北九州市）, 2011 年1 月

19. 橋本康史, 合同部分群に関する*length spectrum* の重複度について, 2011 年度日本数学会年会函数論分科会, 早稲田大学, 2011 年3 月.

〔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〕

６．研究組織
(1)研究代表者
橋本 康史（Yasufumi Hashimoto）
財団法人九州先端科学技術研究所・情報セキュリティ研究室・研究員
研究者番号：30452733

(2)研究分担者
なし

(3)連携研究者
なし