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　３０　年　　５　月　３１　日現在

機関番号：　１７１０２
研究種目：　若手研究(B)
研究期間：　2015～2017
課題番号：　１５Ｋ１７５１５

研究課題名（和文）計算機数論による楕円曲線とモジュラー形式の保型性の研究

研究課題名（英文）On the modularity of elliptic curves and modular forms from a viewpoint of computational number theory

研究代表者

横山　俊一（Yokoyama, Shunichi）

九州大学・数理学研究院・助教

研究者番号：９０７４１４１３

交付決定額（研究期間全体）：（直接経費）　　1,900,000円

研究成果の概要（和文）：楕円曲線とモジュラー形式の双方の計算理論について，保型性による性質の伝搬をヒントとした高速計算理論について，幾つかの成果を得た．楕円曲線側では，主として代数体上の特定の楕円曲線の族を高速に得るためのアルゴリズムの改良を行ったほか，与えられた導手（conductor）をもつ楕円曲線の逆引きアルゴリズムの効率化を得た．一方モジュラー形式側では，主として楕円モジュラー形式の高速計算理論の精密化と，これに伴う Hecke 体の効率的な計算を進めた．また本研究で得られた成果・実装を援用し，楕円曲線暗号（ペアリング暗号）の研究においても成果を与えた．

研究成果の概要（英文）：According to this research project, we provided some fast implementation to compute several family of elliptic curves over algebraic number field, and elliptic modular forms with associated Hecke algebra. More precisely, we achieved to get two efficient algorithm: (i) Searching all elliptic curves having everywhere good reduction with given conductor, and (ii) Calculating maximal orders of Hecke algebra with prescribed ramification of primes over the rational field. In addition, using several refinements by this project, we get an implementation of pairings (from elliptic curves) at the high security bit levels.

研究分野：　計算機数論

キーワード：　楕円曲線　モジュラー形式　高速計算

１．研究開始当初の背景

保型性（modularity）とは、現代数論の中で特に重要な研究対象とされている、次の 2 つを結びつける性質のことである。歴史的にはまず有理数体上の場合で定式化された。
・楕円曲線（elliptic curve）：有理数体上の 3 次曲線で、特異点をもたないもの。
・モジュラー形式（modular forms）：複素上半平面上の正則関数で、特別な変換を保つもの。
とくに有理数体上の保型性を予想した「谷山-志村予想」は非常に有名であり、Wiles による Fermat 予想の解決を皮切りに 2000 年代に入って証明がなされた。その後も Serre 予想や佐藤-Tate 予想といった難予想が次々と解決をみた。近年においてはこれらの一般化が重要視されており、数多くの部分的な結果が得られつつある。

２．研究の目的

本研究では主として、ある代数体上の保型性に関して、計算機数論の観点から考察を行うことを目的とした。とくに計算機を援用することで、明示的なデータを基に楕円曲線とモジュラー形式、および付随する数論的対象物の性質を明らかにできるのではないかと考えた。また得られたデータは数論統合データベース LMFDB を始めとする、オープンなフォーマットで公開し、広く利用してもらうことを目指した。

３．研究の方法

具体的な部分問題を設定して研究を進める。具体的には以下の通り進めた：
【楕円曲線】総実でない基礎体上良い還元をもつ楕円曲線の決定を行う効率的なアルゴリズムの開発とその実装に取り組んだ。例えば、コホモロジー的定義が計算のボトルネックとなっている虚二次体上のモジュラー形式について、楕円曲線側のデータベースを充実させることで幅広く調べた。また従来から申請者によって得られている有理点探索アルゴリズムのさらなる改良を行った。
【モジュラー形式】Edixhoven-Couveignes らによる楕円モジュラー形式の高速計算理論に関して、より効果的な実装の実現可能性について考察した。また、楕円モジュラー形式に付随して、固有形式から定まる Hecke 体と素数の分岐に関する膨大なデータを収集し、前田予想の検証に取り組んだ（その際、楕円曲線側の還元の様子を重要なヒントとして用いる）。ここではボトルネックとなる整環（maximal order）の高速計算も部分問題として設定されており、数式処理の範疇で高速・効率化を試みた。
本研究では、具体的に基礎体を指定し、申請者によって得られたアルゴリズムを改良・最適化することにより、短期間でも新規なデータを得られるようにしている。先行研究においては汎用アルゴリズムの開発に重点が置かれており、利用範囲が高く有用であるが、計算効率の観点から特定の予想の解決に向けたアルゴリズムの開発には利用できなかった。本研究ではあえてこの部分に力を注ぎ、特別な代数体上の保型性を保証するデータを数多く収集する。そして、この成果を広く発信することによって、計算機数論の専門・非専門に関わらず、協力して保型性の解明を進めていくことができると考える。

４．研究成果

【楕円曲線】数論統合データベース LMFDB に対して、代数体上至る所良い還元をもつ楕円曲線の最新のデータを提供した。これは ecegr パッケージとして既に GitHub 上で公開されており、LMFDB への組み込み作業中である。また追加データとして、悪還元をある程度許容した特別な楕円曲線のデータベース化を進めており、一部を同じく LMFDB へ提供した。
この一連の研究成果の一部は、2017 年に計算代数システム Magma が正式に内部関数として採用した EllipticCurveSearch の改良に用いられている。また一部の高速実装は、外部委託共同研究（楕円曲線暗号・ペアリング暗号）において援用された（共同研究契約のルール上詳細は割愛する）。
【モジュラー形式】楕円モジュラー形式の高速計算に用いられるいくつかのサブルーチンの効率化を行った。これらの成果は 2017 年に開催された「第 25 回整数論サマースクール」において公開した他、現在も整備を進めている。とくに Frobenius 元の特定アルゴリズムについては、本質的に多変数多項式の終結式の高速計算に帰着されるため、従来申請者によって得られた実装を更に改良して適用した。
また前田予想に関しては、当初の最終目標であった証明の達成には及ばなかったが、整環計算のボトルネック解消に向けていくつかの手法を得た。これについては 2018 年度以降も継続して行う予定である。

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　6　件）

1. 馬渕圭史、横山俊一、齋藤恆和「BLS 曲線における Optimal Ate Pairing の実装と評価」2018 年暗号と情報セキュリティシンポジウム（SCIS2018），電子出版，6pp.（USB 媒体で公開されているため DOI/URL なし），査読なし.
2. 横山俊一「SageMath Inc. と LMFDB に関

する最近の話題」、2016 年早稲田数論研究集会報告集（2016），pp.139-146.（電子出版ではないため DOI/URL なし：ただし筆者による pdf が http://www2.math.kyushu-u.ac.jp/~s-yokoyama/files/Waseda2016.pdf にある），査読なし.
3. 横山俊一「楕円モジュラー形式の高速計算理論入門」、京都大学数理解析研究所講究録別冊、B53（2016），pp.279-304. http://www2.math.kyushu-u.ac.jp/~s-yokoyama/files/bessatsu-revfinal.pdf, 査読あり.
4. 横山俊一「数論データベース LMFDB の開発について」、第 11 回「代数学と計算」報告集（2015），pp.174-178. http://jant.jsiam.org/ac/2015/ac2015_proceedings.pdf, 査読なし.
5. 横山俊一「代数体上至る所良い還元を持つ楕円曲線の決定と数論データベース化プロジェクトへの貢献について」、数式処理 Vol.21, No.2（2015），pp.41-44. http://www2.math.kyushu-u.ac.jp/~s-yokoyama/files/2014TokushimaJSSAC.pdf, 査読なし.
6. 横山俊一、竹森翔「数式処理におけるモジュラー形式の実装について」、日本応用数理学会論文誌 Vol.25, No.3（2015），pp.207-227. DOI:https://doi.org/10.11540/jsiamt.25.3_207, 査読あり.

〔学会発表〕（計 26 件）

1. 馬渕圭史、横山俊一、齋藤恆和「BLS 曲線における Optimal Ate Pairing の実装と評価」、2018 年日本応用数理学会研究部会連合発表会、2018 年 3 月 16 日、大阪大学
2. 横山俊一「Performant and flexible computer algebra systems in number theory」、宮崎大学 MZ セミナー、2018 年 2 月 19 日、宮崎大学
3. 横山俊一「計算機数論における数式処理システムの援用と最近の進展」、広島大学大学院理学研究科・数学専攻 談話会、2018 年 1 月 16 日、広島大学
4. Shunichi Yokoyama, Number theory with Magma: for performant and flexible computation, 3rd Japanese-German Number Theory Workshop, November 20th 2017, Max Planck Institute for Mathematics, Germany.
5. 横山俊一「計算代数システム Magma 入門と最近の話題」、熊本大学理学部数学教室談話会、2017 年 10 月 30 日、熊本大学
6. 横山俊一「計算代数システム Magma 入門と最近の話題」、香川セミナー、2017 年 10 月 28 日、香川大学
7. 横山俊一「特別な楕円モジュラー形式の高速計算理論について」、整数論サマースクール 2017「楕円曲線とモジュラー形式の計算」、2017 年 8 月 29 日、伊香保温泉塚越屋七兵衛
8. 横山俊一「楕円曲線の計算法入門・実践編」、整数論サマースクール 2017「楕円曲線とモジュラー形式の計算」、2017 年 8 月 29 日、伊香保温泉塚越屋七兵衛
9. 横山俊一「Performant and flexible computer algebra systems in number theory」、新潟代数セミナー、2017 年 5 月 19 日、新潟大学
10. 横山俊一「計算代数システム Magma 入門」、東京理科大学理工学部数学科談話会、2017 年 4 月 21 日、東京理科大学
11. 横山俊一「Computing tables of elliptic curves over number fields」、Meeting for Study of Number Theory, Hopf algebras and related topics、2017 年 2 月 14 日、富山大学
12. 横山俊一「計算代数システム Magma 入門」、島根大学松江セミナー、2017 年 1 月 27 日、島根大学
13. 横山俊一「計算機数論入門：良い還元をもつ楕円曲線を例に」、岡山大学理学部数学科セミナー、2017 年 1 月 25 日、岡山大学
14. 横山俊一「Explicit methods to compute elliptic curves and related structures」、愛媛大学代数セミナー、2016 年 8 月 26 日、愛媛大学
15. Shunichi Yokoyama, Explicit methods to compute elliptic curves and related structures, Algebraic Geometry Seminar, August 5th 2016, University of Kaiserslautern
16. Shunichi Yokoyama, Explicit methods to compute number-theoretic objects, Universal Structures in Mathematics and Computing 2016, June 28th 2016, La Trobe University City Campus, Australia.
17. 横山俊一「Development of LMFDB: a database in number theory」、第 20 回早稲田整数論研究集会、2016 年 3 月 23 日、早稲田大学
18. 横山俊一「Development of LMFDB: a database in number theory」、ラングランズと調和解析、2016 年 3 月 10 日、九州大学
19. Shunichi Yokoyama, On elliptic curves with everywhere good reduction over certain number fields, Computational Algebra Seminar, February 18th 2016, University of Sydney, Australia.
20. Shunichi Yokoyama, SageMath Cloud: a guide tour, Open Seminar on Algebra, Combinatorics and Algorithm, January 15th 2016, Pusan National University, Korea.

21. 横山俊一「数論データベース LMFDB の開発について」、第 11 回「代数学と計算」、2015 年 12 月 16 日、首都大学東京
22. 横山俊一「楕円モジュラー形式の高速計算について」、新潟代数セミナー、2015 年 10 月 23 日、新潟大学
23. 横山俊一「統合数式処理システム Sage 入門」、上智大学数学談話会、2015 年 10 月 16 日、上智大学
24. Shunichi Yokoyama, Developments in computer algebra research and collaboration with industry, The 8th International Congress on Industrial and Applied Mathematics (ICIAM2015), August 14th 2015, China National Convention Center, China.
25. 横山俊一「p 進体のアーベル拡大体生成アルゴリズムの高速化について」、日本数式処理学会第 24 回大会、2015 年 6 月 6 日、筑波大学
26. 横山俊一「p 進体の拡大体生成アルゴリズムの高速化について」、熊本大学代数幾何学セミナー、2015 年 5 月 20 日、熊本大学

〔図書〕（計　　件）

〔産業財産権〕

○出願状況（計　　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　　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〕
ホームページ等

６．研究組織
(1)研究代表者
横山 俊一（YOKOYAMA, Shunichi）
九州大学・数理学研究院・助教
研究者番号：90741413

(2)研究分担者
（　　）

研究者番号：

(3)連携研究者
（　　）

研究者番号：

(4)研究協力者
（　　）