【平成24年4月-12月授与分】博士学位論文内容の要旨及び審査の結果の要旨

氏名・(本籍・国籍)	よこ やま しゅんいち 横 山 俊 一 (福岡県)
学 位 の 種 類	博士 (数理学)
学 位 記 番 号	数理博甲第１５０号
学位授与の日付	平成24年10月31日
学位授与の要件	学位規則第４条第１項該当　数理学府　数理学専攻
学 位 論 文 題 目	Creating some databases in computational number theory (計算機数論におけるデータベース生成について)
論 文 調 査 委 員	(主　査)　准教授　田 口 雄一郎 (副　査)　教 授　金 子 昌 信　　准教授　今 野 拓 也 電気通信大学　教 授　木 田 雅 成

論　文　内　容　の　要　旨

本学位論文では、計算機数論における「良いデータベースの生成と提供」を目的として、2 種類の話題について研究を行った。それぞれについて個別に述べる。

【A. 代数体上至る所良い還元を持つ楕円曲線のデータベース化】 本研究は、現代数論において重要視されている「保型性」を観察することに動機を持ち、幾つかの重要な保型形式との対応が示唆されている。しかしながら代数体上の楕円曲線の計算は計算機的困難が数多く残されており、保型性の考察のために具体的な計算例を組織的に得たデータベースの生成・提供が望まれている。著者はこの課題に取り組み、実二次体上至る所良い還元を持つ楕円曲線の存在・非存在を示した既存のデータベースを大幅に更新した (14 ケースに対して完全決定、9 ケースに対して部分的決定)。更に基礎体を実三次体に引き上げた場合についても研究を行い、既存の Bertolini-Canuto による 1988 年の結果 (1 ケースのみの非存在性) を大幅に更新、12 ケースに対して新たに非存在性を完全に決定した (加えて 6 ケースに対して部分的決定を行った)。またこの過程において、純三次体上至る所良い還元を持つ楕円曲線で非自明に構成されるものを初めて構成した。本研究においては数式処理システム Pari/GP, Magma, Sage を併用し、Mordell-Weil 群の計算を数式処理の道具を用いて高速実装することで、通常利用では計算不可能な例を提示することに成功している。なお実二次体上の場合については島崎有氏との共同研究から発展したものである。

【B. 局所体の高速生成アルゴリズムの作成とデータベース化】 本研究は、局所体の Galois 群の高速・効率計算を一つの目標として行われたものである。大域体・局所体に共通してこれまで使用されてきたアルゴリズムは分解式計算を使用するものであり、有用ではあるが高次の場合には機能しないというデメリットを持つ。更に数式処理研究の観点からも局所体計算は大域体計算に比べて計算機的に未発達な部分が多い。そこで著者は数式処理システム Magma に実装されている局所体生成プログラムを高次の場合にも耐えうるよう改良を図った。具体的には p 進体上 1) p 次拡大, 2) 完全分岐アーベル拡大, 3) 低次アーベル拡大 の 3 種類 (但し p は奇素数) の拡大体の高速生成アルゴリズムとその Magma による実装を与えた。更に 1) に関しては p 次 Eisenstein 多項式が定義する拡大体の同型判定アルゴリズムを実装と共に与えた。これは従来広く用いられていた Panayi による root counting アルゴリズムを用いた場合と比較して大幅な高速化に成功している。1), 2) に関しては p を大きくとっても実行可能となっており、更に 3) については拡大次数の p 進付値が 2 以下という制限の下で従来よりも比較的高次の拡大体まで生成出来るようになっている。本研究は吉田学氏との共同研究である。

以上の研究によって得られたアルゴリズムとその実装 (実行可能なプログラム)、及びデータベースは、著者のウェブページにて公開しており、容易に閲覧可能となっている。

論文審査の結果の要旨

本論文に於いては、数論に於いて有用な二種類のデータベースが構築されている。一つは、二次体や三次体上定義された楕円曲線であって至る所良還元（good reduction）を持つもののデータベースであり、もう一つは p 進体の有限次拡大のデータベースである。その計算には Magma を始めとする計算機代数システムが巧みに組合せて用いられており、計算技法の観点から見ても現代的な、高度なものとなっている。

代数体 K とその有限素点の有限集合 S を固定すると、K 上定義された楕円曲線であって S の外で良還元を持つものは有限個しか存在しない事が知られている（これは楕円曲線のみならずより一般にアーベル多様体について成り立つ（Faltings の定理））。「至る所良還元を持つ」とは S が空集合の場合であるから、それらが有限個しか存在しない事は一般論から従うが、実際にそれらを決定する事はまた別問題で、一般にかなりの困難を伴う問題である。K が有理数体の場合はその様な楕円曲線は存在しない事が知られており（これも一般にアーベル多様体について成り立つ(Fontaine の定理)）、K が二次体の場合には、幾つかの K について木田雅成氏や加川貴章氏らによる先行研究があった。本論文では彼らの方法を組織的に押し進め、大量の計算を必要とする箇所では最新の計算機及び計算プログラムを援用する事で、これまで知られていた結果を大幅に拡張した。さらに K が三次体の場合にも独自の方法でこの様な結果を得た。その結果、200 以下の殆どの正整数 m に対し実二次体 $K=\mathrm{Q}(\sqrt{m})$ の場合及び三次体 $K=\mathrm{Q}(m\text{^}\{1/3\})$ の場合に満足の行くデータベースが得られた。各 K について、至る所良還元を持つ楕円曲線が存在する場合にはその楕円曲線の方程式も与えられており、実用的価値も高い。

標数 0 の局所体 K と自然数 n を固定すると、K の n 次拡大は同型を除き有限個しか存在しない事が知られている。従って特に p 進体 $\mathrm{Q}p$ の n 次拡大は有限個であるが、p や n の値が大きくなると、それら全てを実用的な時間内に求める事は容易ではない。p 進体の p 次拡大の標準形を与えた Amano 氏の仕事や Eisenstein 多項式のなす空間にうまい距離を入れてそれらの定義する体たちの間の同型判定法を与えた吉田学氏の仕事に基き、本論文においては、比較的大きい p と n に対し、$\mathrm{Q}p$ の n 次拡大を全て、しかも高速に、求めるプログラムが与えられている。特に、p 進体の n 次拡大のかなり広範なデータベースが得られた。これは Jones や Pauli-Roblot の結果を大幅に改善するものである。さらに特筆すべき事として、このプログラムは著者のホームページにおいて無料で公開され、誰にでも利用可能になっている。

これら二つのデータベースは、著者の「数論データベースプロジェクト」の最初の一歩であり、今後これらがさらに拡張されて行くのはもちろん、他の対象についてのデータベースも生成され、統合されて、一つの大きな、使い勝手の良いデータベースのシステムが構築されて行く事が期待されている。これは膨大な時間がかかる遠大な計画であるが、その一端が本論文の第一章で青写真として素描されている。

この様に、以上の結果は、既に生成された二つのデータベースが数論研究者にとって非常に価値の高い有用なものであると同時に、その発展性や将来的ヴィジョンなどにおいても優れたものであり、数論の分野において価値ある業績と認められる。

よって、本研究者は博士（数理学）の学位を受ける資格があるものと認める。