様式 C-19

科学研究費補助金研究成果報告書

平成 21 年 5 月 29 日現在

研究種目： 若手研究(B)
研究期間： 2006 ～ 2008
課題番号： 18740013
研究課題名（和文） 楕円曲線のセルマー群の計算アルゴリズム開発とその応用

研究課題名（英文） Development of algorithms for the computation of Selmer groups of elliptic curves and its application

研究代表者
松野 一夫（MATSUNO KAZUO）
津田塾大学・学芸学部・准教授
研究者番号：40332936

研究成果の概要： 代数体上の楕円曲線の数論における中心的な研究対象の一つである Selmer 群を具体的に計算するためのアルゴリズムの開発を行った。既存のアルゴリズムを分析し、改良を試みながら、実例計算によるデータの収集を行う一方で、開発中に得られた知見を理論的に応用する考察も行い、代数体上の楕円曲線の Tate-Shafarevich 群の大きさの非有界性や、楕円曲線の 2 進岩澤不変量についての新たな事実の発見といった成果を得た。

交付額

（金額単位：円）

	直接経費	間接経費	合 計
2006 年度	900,000	0	900,000
2007 年度	700,000	0	700,000
2008 年度	700,000	210,000	910,000
年度			
年度			
総 計	2,300,000	210,000	2,510,000

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：楕円曲線、Selmer 群、岩澤理論

１．研究開始当初の背景

種々の数論的対象に付随する Selmer 群や zeta 関数の性質およびそれらの間の結び付きを調べることが整数論の研究における一つの中心テーマとなっているが、代数体上の楕円曲線に付随して定義される Selmer 群は、有理点のなす Mordell-Weil 群や Hasse 原理の成り立たない度合いを示す Tate-Shafarevich 群といった対象の情報をあわせ持つものであり、Hasse-Weil L 関数との結び付きを予想する Birch, Swinnerton-Dyer 予想は現在でも最重要未解決問題の一つとして位置付けられている。その楕円曲線の Selmer 群は、理論的には計算可能なものであり、特に 2 倍写像により定義される 2-Selmer 群の計算については、具体的な計算法が古くから考察され、少なくとも有理数体上の楕円曲線の場合は様々なシステム上で実際に計算が可能な状態であった。計算機の能力向上に伴い、以前は不可能であったような代数体上の諸量の計算が可能になってきたことも受け、奇素数 p に対しても p-Selmer 群の計算を

行うプログラムの開発が望まれる状況となり、Cremona, Fisher, Schaefer, Stoll といった研究者らにより、新しい計算アルゴリズムが提案されつつあった。しかし、当時、それらの研究は始まったばかりで、特別な具体例だけではなく幅広い計算を行えるような計算機への実装はまだなされておらず、理論的な側面でも例えば局所条件の具体的記述など、改良すべき点が多く残されていた。
Euler 系を利用し、L 関数の特殊値によって Selmer 群の大きさを上から評価するという研究も Kolyvagin 以降大きく発展し、Birch, Swinnerton-Dyer 予想との関係もあって非常に重要であるが、自明になる場合を除いて Selmer 群を完全に決定できるものではなく、また、それを Selmer 群や Tate-Shafarevich 群の具体的計算に直ちに利用できる形で実装している計算システムはほとんどなかった。楕円曲線の岩澤理論の諸結果により、p 進 L 関数を使った Selmer 群の評価も具体的計算に有効であるが、そのような計算も多くは行われていなかった。

２．研究の目的

一般の有限次代数体上で定義された楕円曲線に付随する Selmer 群を計算するための理論やアルゴリズムの開発、計算機への実装、およびそれらを活用した楕円曲線に関する諸問題の検証、考察を行うことを目的とする。Selmer 群の具体的計算は楕円曲線についての予想の考察や新たな現象の発掘に非常に重要であるため、既存のアルゴリズムの改良や新しいアルゴリズムの開発を行い、計算データを集めることはそれ自体意味あるものであるが、本研究ではそれだけでなく、得られた Selmer 群の表示を代数体上の楕円曲線の Tate-Shafarevich 群や岩澤不変量の性質の理論的考察に応用することも目的としている。具体的には

・Schaefer-Stoll の Selmer 群計算アルゴリズムの改良・拡張およびその実装
・Selmer 群の計算アルゴリズムの楕円曲線の岩澤理論への応用
・楕円曲線の p 進 L 関数の計算と Birch, Swinnerton-Dyer 予想の検証
・大きな Selmer 群や Tate-Shafarevich 群を持つ楕円曲線の構成
・代数体と関数体の類似を踏まえた上での実例計算や諸予想の検証

などを主なテーマとして考察を行う。

３．研究の方法

・楕円曲線の Selmer 群を計算するアルゴリズムの理論的な考察および開発
・各種アルゴリズムの計算機への実装と実例計算によるデータ収集
・Selmer 群計算の新しいアルゴリズムの理論的な応用の探求

を 3 つの柱として、それらを独立に進めるのではなく、同時並行的に研究を進め、部分的にでも得られた成果をすぐに他の方向にも展開させる方法を取る。具体的には、Schaefer と Stoll による楕円曲線の Selmer 群計算アルゴリズムの分析と改良の考察から始め、その Selmer 群の表示を利用して八森による楕円曲線の岩澤 μ 不変量とある 3 次体の一部分岐岩澤加群の μ 不変量との関連についての結果の別証明を与える。更に p 進 L 関数の計算によるデータ収集を行って Tate-Shafarevich 群や岩澤不変量の振る舞いなどを観察しながら、八森の結果の p=2 の場合への一般化の考察や、大きな Tate-Shafarevich 群を持つ楕円曲線の構成などへと繋げていく。

４．研究成果

(1) p が 7 以下の素数または p=13 の場合に、有理数体上に定義された楕円曲線の岩澤 λ 不変量が非有界であることおよび、有理数体上の Tate-Shafarevich 群の p-階数も非有界であることを証明した。Tate-Shafarevich 群の p-階数の非有界性については、同種写像による Selmer 群の変化に関する Cassels の古典的な結果と楕円曲線の L 関数の特殊値についての Waldspurger らによる結果を組み合わせることで証明できることが、本研究開始前にわかっていたのであるが、楕円曲線の岩澤不変量についての考察を進める中で、得られた λ 不変量の非有界性についての結果と Mazur の制御定理を組み合わせることで、別証明を与えることが出来ると気付き、それらをまとめて一つの論文とし、出版した(発表論文③)。岩澤 λ 不変量の非有界性の証明自体は、Greenberg による様々な結果に Waldspurger の結果を組み合わせるというもので、それほど驚くべきものではないと思われるが、うまい twist の選び方など細かな注意が必要なところもあり、実際の証明はやや複雑である。
Tate-Shafarevich 群の p-階数の非有界性については、p=7, 13 の場合がそれまでに知られていなかったのであるが、p=7 に関しては同時期に Steve Donnelly が同様の結果を独立に得ていたとのことである(論文未発表)。し

かし、Donnelly の結果を知る国外の研究者の論文に「11 以上の素数に対しては、現行の方法では乗り越えることのできない困難があるように感じられる」と記されていたように、13-階数に対しても同様の結果が得られることは、類似の研究を行っている研究者にとっても驚きであったようである。(2)に述べる結果と合わせて、この分野の専門家にとってはかなり興味深い結果であったと考えられる。

(2) 任意の素数 p と任意の p 次巡回拡大体 K に対し、K 上の Tate-Shafarevich 群の p-階数が任意に大きな値を取る有理数体上の楕円曲線を構成することが出来た。(1)では小さな素数 p に対して有理数体上での非有界性を証明したのであるが、こちらは素数を任意にする場合でも体を少し拡大すればやはり非有界性が示せるというものであり、(1)の一つの拡張と言える。有理数体上での非有界性を任意の素数の場合に拡張するのは非常に困難であるとの認識の下、定義体と楕円曲線の両方を動かして非有界性を示す試みは以前から行われており、p^5次以下の代数体とその体上の楕円曲線を全て動かせば可能であるということが、Remke Kloosterman によって示されていた。今回の結果はこの拡大次数を p 次に下げただけでなく、体の方は任意に固定して良いとした点で、知られていた結果の大幅な改良を与えたことになる。この結果をまとめた論文(発表論文①)はまだ出版されていないこともあり、近い研究を行っている国外の複数の研究者から内容の問い合わせを受けたが、ここまでの改良が出来るとは想像していなかった様子であった。
有限次代数体上での結果であるが、岩澤理論の考察を発展させて得た結果であり、証明でも岩澤理論における Mazur の制御定理の類似物を示し、利用している。Selmer 群の情報から Tate-Shafarevich 群の情報を取りだすところは篩の理論の古典的な結果を利用した。どちらの手法も専門家にはよく知られたものであるが、それらを組み合わせる部分はかなり技巧的なところもあり、今後、類似の研究で利用されることもあるのではないかと考えている。

(3) 楕円曲線の岩澤 λ 不変量に対する木田の公式の類似を p=2 の場合に拡張した。木田の公式とは古典的な岩澤 λ 不変量が体の拡大でどのように変化するかを記述する公式であるが、以前に楕円曲線の岩澤不変量に対する類似の公式を八森との共同研究で示していた。しかし、p=2 の場合は定義体が総虚であるという仮定を置いており、その仮定を外したのが今回の結果である。Cohomology の計算がかなり複雑になる以外は以前と同様の議論が行えるため、新しい結果と言うよりは、残されていた部分を補完するという意味合いの強い結果ではあるが、p=2 の場合特有の現象も見つかっており、発表の価値は十分にあると考える。また、それを主目的としていたのであるが、p=2 の場合の木田の公式は λ 不変量の twist による変化と密接に関係しており、副産物として(1)で示した λ 不変量の非有界性の p=2 の場合の別証明も得られる。実際にはより強く、λ 不変量が任意の非負整数値を取り得るということを証明した。
以前に示した結果の拡張ということもあり、結果の一部は本研究の開始前に既に得ていたのであるが、Selmer 群の別表示の考察などを通じて結果を整理し、更に p=2 の場合の岩澤 λ 不変量についてのいくつかの注意などもまとめて出版した(発表論文②)。

(4) Schaefer-Stoll の Selmer 群計算アルゴリズムの分析と考察を行う中で、楕円曲線の岩澤 μ 不変量の研究への応用の考察も行い、八森による p=3 の場合の μ 不変量に関する結果の類似を p=2 の場合へと拡張することを試みた。八森の結果は可約 mod p Galois 表現を持つ楕円曲線の岩澤 μ 不変量についての Greenberg による結果を補完するもので、楕円曲線の μ 不変量をある 3 次体の「一部分岐岩澤加群」の μ 不変量と関係づけている。この一部分岐岩澤加群は、古典的な岩澤理論での考察対象と言うべきものであるが、これまであまり詳しく調べられていなかったものである。本研究では p=2 の場合に正判別式の楕円曲線に対して同様の考察を行い、類似の結果を得た。p=3 の場合と比べ、Selmer 群自体の扱いは容易になるが、一部分岐岩澤加群の方は実素点の分岐まで考慮しなくてはならず、その μ 不変量は新しい研究対象と言えると思われる。その後更に、mod p 表現が既約となる場合にも同様の考察を行い、部分的な結果を得ている。今後も引き続き研究を続け、(5)に述べる p 進 L 関数の計算結果もあわせることで、μ 不変量についての更に深い理解を得ることを目指している。

(5) ordinary reduction を持つ楕円曲線の p 進 L 関数を計算するプログラムを計算代数システム MAGMA 上に実装し、岩澤不変量等の計算を行った。以前にも、pari のライブラリを一部利用したプログラムを作成し同様の計算を行っていたが、楕円曲線や保型形式に関するコマンドが近年特に充実してきている MAGMA 上で計算を行えるようにすることは、Selmer 群計算への利用を考える上でも重要である。Pollack による overconvergent modular symbol を利用した p 進 L 関数の新しい計算法の実装は間に合わなかったが、それも含め、今後さらに改良を加え、より幅広い

データの収集を行いたいと考えている。なお、同様の計算プログラムは Chris Wuthrich も開発を行っているが、本研究で作成したプログラムは岩澤理論的な応用をより強く念頭に置いており、計算対象が完全に重なる訳ではない。計算結果についての情報交換などで連携を取りながら、得られたデータを有意義に活用できる形にしていきたい。2010 年にカナダで行われる p 進 L 関数についての研究集会でも、この周辺の成果を発表する予定である。

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 3 件）
① Kazuo Matsuno, Elliptic curves with large Tate-Shafarevich groups over a number field, Mathematical Research Letters 誌に掲載予定, 査読あり
② Kazuo Matsuno, On the 2-adic Iwasawa invariants of ordinary elliptic curves, International Journal of Number Theory, 4, 403-422, 2008 年, 査読あり
③ Kazuo Matsuno, Construction of elliptic curves with large Iwasawa λ-invariants and large Tate-Shafarevich groups, Manuscripta Mathematica, 122, 289-304, 2007 年, 査読あり

〔学会発表〕（計 1 件）
① 松野 一夫, 楕円曲線の岩澤不変量と一部分岐岩澤加群, 室蘭数論研究集会, 室蘭工業大学, 2006 年 10 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〕
ホームページ等

６．研究組織
(1)研究代表者
松野 一夫（MATSUNO KAZUO）
津田塾大学・学芸学部・准教授
研究者番号：40332936

(2)研究分担者
なし （ ）

研究者番号：

(3)連携研究者
なし （ ）

研究者番号：