科学研究費助成事業　　研究成果報告書

平成　２６　年　　６　月　　２　日現在

機関番号：３２６４２
研究種目：若手研究(B)
研究期間：2010～2013
課題番号：２２７４００２４

研究課題名（和文）Ｔａｔｅ‐Ｓｈａｆａｒｅｖｉｃｈ群の計算法開発とその応用

研究課題名（英文）Development of an algorithm for the calculation of the Tate-Shafarevich groups and a pplicaiton

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

交付決定額（研究期間全体）：（直接経費）　　2,700,000円、（間接経費）　　810,000円

研究成果の概要（和文）：有理数体とは限らない有限次代数体上の楕円曲線のTate-Shafarevich群の計算法を開発するとともに、データの収集を行った。また、楕円曲線の2進岩澤μ不変量とある代数体の一部分岐岩澤加群の関連を利用し、μ不変量に関するGreenbergの予想および楕円曲線の2進岩澤主予想を広範囲に実例で検証した。代数体上の楕円曲線のMordell-Weil群のrankが取り得る値に関しても新たな例を発見した。

研究成果の概要（英文）：We develop an algorithm for the calculation of the Tate-Shafarevich groups of elliptic curves defined over number fields. We also make a numerical verification of a conjecture by Greenberg for 2-adic Iwasawa mu-invariants of elliptic curves and 2-adic Iwasawa main conjecture for elliptic curves by using a relation between mu-invariants of elliptic curves and partly ramified Iwasawa modules associated with certain number fields. Moreoer, we find some examples related to the problem about the rank of the Mordell-Weil group of elliptic curves over number fields.

研究分野：代数学

科研費の分科・細目：数学・代数学

キーワード：整数論　楕円曲線　Tate-Shafarevich群

１．研究開始当初の背景

種数が１の非特異代数曲線であり、また１次元のアーベル多様体でもある楕円曲線は、整数論や数論幾何における最も基本的かつ魅力的な研究対象であるが、暗号理論との関連やWilesらによる谷山志村予想の解決などを受けて、近年、ますます注目され、研究されている。代数体上で定義された楕円曲線に付随するTate-Shafarevich群は、種数が１の曲線において「Hasse原理」が成り立たない度合いを測るものであり、代数体上の楕円曲線の局所自明なtorsorの同型類全体が作るアーベル群のことである。代数的整数論におけるイデアル類群の類似物とみなせるものであり、単数群の類似物にあたるMordell-Weil群と並び、代数体上の楕円曲線の数論における中心的な研究対象である。また、それらとHasse-Weil L関数との結び付きを予想するBirch, Swinnerton-Dyer予想は、整数論のみならず、現代の数学における最重要未解決問題の１つとして位置付けられている。しかしながら、このBirch, Swinnerton-Dyer予想の一部として含まれる、Tate-Shafarevich群は常に有限群であるという基本的な予想すら一般に解決には程遠い状況にあり、Birch, Swinnerton-Dyer予想の最も難しい部分であるとも考えられている。

個々の楕円曲線のTate-Shafarevich群を計算する方法としては、降下法により楕円曲線の同種写像に付随するSelmer群を計算し、更にMordell-Weil群に属する有理点の探索を行うことなどによりTate-Shafarevich群の情報を分離するというアプローチが古くから知られていた。しかし、机上の理論としてではなく現実的に利用可能な方法が与えられるようになったのは、2倍写像に付随するSelmer群の計算を除いてはごく最近のことであり、まだ十分な考察・検討が行われているとは言えない状況であった。また、有理数体ではない一般の代数体上では、理論的な側面での研究もほとんど行われていないというのが実情であった。

２．研究の目的

整数論における極めて重要な研究対象である有限次代数体上の楕円曲線に付随するTate-Shafarevich群の計算法の開発・改良を、楕円曲線の岩澤理論における手法や諸結果も活用しながら行うとともに、実例計算によるデータの収集を広範に行う。さらに、その過程で得られた新たな知見も踏まえつつ、代数体の拡大における変化の様子の考察など、有理数体とは限らない一般の代数体上におけるTate-Shafarevich群の性質についての理論的な考察をしていくことも研究の目的の一つとする。具体的には

・Schaefer-Stoll、Fisherらのアルゴリズムによる楕円曲線のSelmer群の計算アルゴリズムをベースとした、Tate-Shafarevich群の計算プログラムの開発、実装

・楕円曲線の岩澤理論に関する諸結果を利用した、有限次代数体上の楕円曲線のTata-Shafarevich群の計算法の開発および計算

・楕円曲線の岩澤不変量および岩澤主予想についての考察、特に2進岩澤μ不変量の考察および2進岩澤主予想の検証

・Tate-Shafarevich群の単項化と可視性についての考察

などを主なテーマとして研究を行い、新たな知見を得ることを目的とする。

３．研究の方法

有理数体とは限らない有限次代数体上に定義された楕円曲線のTate-Shafarevich群について、計算機も活用した研究・開発を行う。具体的には研究の目的に挙げた内容を

・Tate-Shafarevich群の計算に関する既存の方法の改良、新たな手法の開発

・Tate-Shafarevich群の計算アルゴリズムの計算機への実装、データ収集

・計算データから観察された現象の理論的裏付け

・Tate-Shafarevich群に関する問題の実験的検証と理論的考察

と分けて実行した。ただし、それぞれを分離して独立に進めるのではなく、実験的な部分と理論的な部分の研究を並行して行い、効率的に研究を進めた。具体的には、楕円曲線の2進岩澤μ不変量に関する計算と、それを活用し、2進岩澤主予想の検証を行うところから研究を始め、Fisherらの Selmer群の計算アルゴリズムに基づくTate-Shafarevich群の計算プログラムの開発・実装を行いながら、理論的な考察への応用を検討していった。

４．研究成果

(1)　有理数体上定義された楕円曲線の2進岩澤μ不変量の計算を広範に行った。素数pに対し、Galois群がp進整数環の加法群Zpと同型であるような有理数体のただ１つの拡大(もしくはそれと代数体との合成体)を円分Zp拡大と呼ぶが、楕円曲線の岩澤不変量とは円分Zp拡大におけるSelmer群の変化を記述する不変量であり、特に岩澤μ不変量はTate-Shafarevich群の変化のみに関係する不変量である。2でgood ordinary reductionを持つ楕円曲線の2進岩澤μ不変量(p=2の場合の不変量)と、ある代数体の一部分岐岩澤加群のμ不変量との間に密接な関係があることを既に示していたが、本研究ではその一部分岐岩澤加群を円単数なども利用して調べることにより、μ不変量の実例計算を実行した。一部分岐岩澤加群の計算がとても困難な場合もあったが、位数2の有理点を持ち導手が5000未満の楕円曲線などについて、Greenbergによるμ不変量に関する予想が成立することを確認した。

(2) 有理数体上定義された楕円曲線の2進岩

澤主予想の幅広い検証を行った。素数 p で ordinary reduction を持つ有理数体上の楕円曲線に対し、有理数体の円分 Zp 拡大における楕円曲線の Selmer 群の変化と、楕円曲線の p 進 L 関数の間に密接な関係があるとする岩澤主予想は、楕円曲線の岩澤理論における中心的な予想である。予想の半分にあたる部分が正しいことを示す加藤の結果以降しばらく大きな進展はなかったのであるが、Skinner-Urban により、いくつかの仮定の下で予想は正しいことが最近示された。その仮定の多くは深刻ではない条件であるが、残念ながら p が奇素数の場合しか扱われておらず、p=2 の場合には主予想は未解決である。その p=2 の場合には八森との共同研究で得られた楕円曲線の岩澤λ不変量に対する木田の公式の類似と、岩澤主予想についての加藤の結果を組み合わせることにより、μ不変量についての Greenberg の予想が正しいという仮定のもとで楕円曲線の岩澤主予想を検証することができるのであるが、(1)のμ不変量に関する予想を検証した範囲のすべての曲線で主予想も成立することを、2 進 L 関数の具体的な計算により確認した。なお、μ不変量の計算の方が困難な場合が多いため、今後、μ不変量についての予想の検証を進められれば、主予想も同時に検証可能であると期待される。計算には Magma 上に実装した楕円曲線の p 進 L 関数を求めるプログラムを用い、対象となる曲線やその 2 次 twist に対して各種の不変量を計算することで結果を得た。この検証結果については、(1)の 2 進岩澤μ不変量と一部分岐岩澤加群との関連を考察した結果とともに論文にまとめているところである。

(3) 有理数体とは限らない有限次代数体上に定義された楕円曲線の Tate-Shafarevich 群を求める計算法の開発および実例計算を行い、データを収集した。Tate-Shafarevich 群はその定義により Selmer 群と密接に関係しているため、まずは Selmer 群の計算を行うことになるが、Schaefer-Stoll や Fisher らによる Selmer 群計算アルゴリズムは有理数体ではない一般の代数体上で自由に利用できる状態にはなかったため、必要な事柄を検証しつつ計算機への実装を試みるとともに、可能な範囲で計算を行って Tate-Shafarevich 群のデータを収集した。また、Selmer 群から Tate-Shafarevich 群のデータを得るためには Mordell-Weil 群を考察する必要があるが、直接計算を試みるだけでなく、岩澤理論からの結果、特に岩澤主予想に関する加藤の結果を利用し、p 進 L 関数の計算で Mordell-Weil 群の大きさを評価することも試みた。p 進 L 関数の定義、計算には modular symbol を利用するが、栗原による楕円曲線の Tate-Shafarevich 群の modular symbol を用いた最新の計算法に関する実例計算も行った。一般に計算機による modular symbol の計算は非常に多くのメモリを必要とするため、大きな導手の曲線を扱うのは難しいのであるが、今回購入した計算機を利用することで、新たな興味深い具体例の計算を実行できた。

(4) 楕円曲線の Tate-Shafarevich 群の計算法開発が本研究の中心的なテーマであるが、それと密接に関係する、有理数体とは限らない代数体上の楕円曲線の Mordell-Weil 群の計算も行い、新たなデータを得ることができた。楕円曲線の Mordell-Weil 群の rank については、少なくとも定義体や曲線を動かすことを認めれば、任意の非負整数値を取り得ると期待される。楕円曲線に関するいくつかの基本的な予想の下では正しいことが最近の Mazur-Rubin の結果を使って示せるが、予想を仮定せずに与えられた非負整数を rank にもつ楕円曲線を実際に見つけるのは容易ではない。有理数体上では 19 以下の非負整数を rank にもつ楕円曲線の具体例が見つかっているが、それ以上の整数を rank にもつような楕円曲線を有理数体とは限らない代数体上で探した計算例は見当たらなかったため、計算を行い、例えば 100 以下の偶数であれば rank として現れることなどを確認した。また、導手が 1 となる代数体上の楕円曲線の Mordell-Weil 群の rank の偶奇性予想についても関連する計算を行った。

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　1　件）

1．松野 一夫，代数体上の楕円曲線の計算と Magma，Magma で広がる数学の世界，Math-for-Industry COE Lecture Note，Vol. 29，pp.134-144，2010 年，査読なし

〔学会発表〕（計　4　件）

1．松野 一夫，楕円曲線の Mordell-Weil 群について，北陸数論研究集会，金沢大学サテライトプラザ，2013 年 12 月 27 日
2．松野 一夫，2 等分点をもつ楕円曲線の岩澤μ不変量の計算，九州代数的整数論 2012，九州大学，2012 年 2 月 22 日
3．松野 一夫，岩澤λ不変量の Riemann-Hurwitz 公式とその周辺，北陸数論研究集会，金沢大学サテライトプラザ，2010 年 12 月 27 日
4．松野 一夫，代数体上の楕円曲線の計算と Magma，Magma で広がる数学の世界，九州大学，2010 年 10 月 10 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〕
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：