2版

様　式　C－19、F－19、Z－19　（共通）

科学研究費助成事業　　研究成果報告書

平成２８年　６月　２日現在

機関番号：３２６６５

研究種目：基盤研究(C)（一般）

研究期間：2013～2015

課題番号：２５４０００２５

研究課題名（和文）楕円曲線の有理点と整数点，および関連する不定方程式の研究

研究課題名（英文）Rational points and integer points on elliptic curves and the related Diophantine equations

研究代表者

藤田　育嗣（FUJITA, Yasutsugu）

日本大学・生産工学部・准教授

研究者番号：５０５１４１６３

交付決定額（研究期間全体）：（直接経費）　　2,900,000円

研究成果の概要（和文）：本研究では，(1)整数係数の方程式で定義された楕円曲線の有理点群の生成元や整数点を調べる(2)ディオファンタスの2組の5組への拡張可能性を調べる の2つの目的を遂行した．(1)について，楕円曲線$C_m: x^3+y^3=m$（mは3乗因子をもたない）に対しC_mの有理点群の階数が1，2の各場合に生成元および整数点を決定した．また楕円曲線$E^N: y^2=x^3-N^2x$ について，E^Nの有理点群の階数が2や3の場合に生成元を具体的に調べた．(2)について，$a<b<a+4\sqrt{a}$や$b<3a$を満たすディオファンタスの2組$\{a,b\}$はディオファンタスの5組に拡張できないことを示した．

研究成果の概要（英文）：Our purpose of this research are (1) to study the generators and integer points on elliptic curves defined by equations having integral coefficients, and (2) to examine the extensibility of Diophantine pairs to Diophantine quintuples. For (1), let C_m be the elliptic curve defined by $x^3+y^3=m$, where m is cube-free. Then we determined the generators for the group $C_m(Q)$ of rational points on C_m and integer points on C_m in the cases where $C_m(Q)$ has rank 1 or 2. Moreover, we explicitly investigated the generators for the group $E^N(Q)$ of rational points on E^N defined by $y^2=x^3-N^2x$ in the case where the rank of $E^N(Q)$ is 2 or 3. As for (2), we showed that any Diophantine pair $\{a,b\}$ satisfying $a<b<4\sqrt{a}$ or $b<3a$ cannot be extended to a Diophantine quintuple.

研究分野：数物系科学

キーワード：楕円曲線　不定方程式　モーデルヴェイユ群　生成元　整数点　連立ペル方程式

1．研究開始当初の背景

(1) 整数係数の方程式で定義された楕円曲線 E に対し，Mordell の定理より E の有理数体 $\mathbb{Q}$ 上の有理点のなす群 $E(\mathbb{Q})$ は有限生成アーベル群であり，そのねじれ部分群を決定することは容易であるが，自由部分群については，階数を決定することすら一般には容易ではない．

また，Siegel の定理より E の整数点は高々有限個であり，Baker によって整数点の個数の上限が明示的に与えられているが，その上限は非常に大きく，整数点を決定することはやはり一般には容易ではない．

① Fermat の 3 次式の 3 次 twist $x^3+y^3=m$（m は 3 乗因子をもたない整数）で定義される楕円曲線 C_m に対し，Everest, Ingram, Stevens は，$C_m(\mathbb{Q})$ の階数が 1 ならば C_m の整数点は高々2 つであり，しかもそのうちの 1 点が $C_m(\mathbb{Q})$ の生成元に入ることを示した（Everest-Ingram-Stevens，2009 年）．証明には elliptic divisibility sequence が使われている．

研究代表者は，標準的高さ (canonical height) を精密に計算することにより上記 Everest らの結果の簡明な別証明が与えられるであろうことに気づいた．また，$C_m(\mathbb{Q})$ の階数が 2 の場合にも，$C_m(\mathbb{Q})$ の生成元や C_m 上の整数点が決定できるのではないかと考えた．

② 研究代表者は寺井伸浩氏と共に，「無限に多くの」正整数の無限族 n に対し $E: y^2=x^3-nx$ （n は 4 乗因子をもたない正整数）の形の楕円曲線の有理点群 $E(\mathbb{Q})$ の自由部分群のある 2 点が $E(\mathbb{Q})$ の生成元に入ることを示した（Fujita-Terai，2011 年）．さらに研究代表者は，n に関する条件を 1 つ付け加えることにより，様々な無限族 n に対してある 3 点が $E(\mathbb{Q})$ の生成元に入ることを示した（Fujita，2013 年）．

上記の楕円曲線 E において，n は平方数とはならないが，合同数 N に伴う楕円曲線 $E^N: y^2=x^3-N^2x$ に対しても，階数が 2 および 3 の場合に $E^N(\mathbb{Q})$ の生成元が決定できるような無限族 N の表示が見つかるのではないかと考えた．

(2) 相異なる正整数の集合 $\{a_1,\cdots,a_m\}$ は，すべての $i\neq j$ に対し a_ia_j+1 が平方数であるときディオファンタスの m 組であると呼ばれる．古くからディオファンタスの 5 組は存在しないという予想がある．ディオファンタスの 6 組は存在せず，ディオファンタスの 5 組は高々有限個しか存在しないこと（Dujella，2004 年）や，ディオファンタスの 2 組 $\{k-1,k+1\}$ はディオファンタスの 5 組に拡張できないこと（Fujita, 2008 年）などが知られている．

研究代表者は，2 つの代数的数の対数の 1 次形式に関する Baker の方法と Rickert による連立有理数近似（Rickert，1993 年）の改良を利用すれば，上で述べた後者の結果を一般化できるのではないかと考えた．

2．研究の目的

(1)
① 楕円曲線 $E_m: y^2=x^3-432m^2$ 上の有理点の標準的高さを局所的高さを使って計算することにより，$C_m: x^3+y^3=m$ の有理点群の階数が 1 や 2 の場合に，生成元や整数点を調べる．

② 正整数 N がある条件を満たすとき，楕円曲線 $E^N: y^2=x^3-N^2x$ について，局所的高さ（local height）を利用して標準的高さを明示的に評価することにより，E^N の有理点群 $E^N(\mathbb{Q})$ の階数が 2 や 3 の場合に，$E^N(\mathbb{Q})$ の生成元を調べる．

(2) まず Rickert による連立有理数近似を我々の状況において改良したものを用いて，与えられたディオファンタスの 2 組 $\{a,b\}$ $(a<b)$ に対し，$\{a,b,c\}$ $(b<c)$ がディオファンタスの 3 組となるような最小の c の上限を求める．次に，2 つの対数の 1 次形式に関する Baker の方法を用いて，様々な無限に多くのディオファンタスの 2 組 $\{a,b\}$ に対し，$\{a,b\}$ がディオファンタスの 5 組に拡張できないことを示す．

3．研究の方法

(1)
① C_m 上の整数点 P の E_m における像 P' の標準的高さを評価することと $E_m(\mathbb{Q})$ 上の無限位数の点の標準的高さの一様な下限を求めることにより，C_m の階数が 1 の場合に整数点が高々2 つであることを示す．標準的高さの評価には，Silverman による局所的高さを計算するためのアルゴリズム（Silverman, 1988 年）を利用する（標準的高さは局所的高さの和として計算することができる）．また，階数が 2 の場合には $m=a^3+b^3=c^3+d^3$（$a,b,c,d\in\mathbb{Z}$）と表されると仮定して，同様に生成元を決定する．なお，このように表される a,b,c,d の例として，例えば

$a=4u^2-4uv+6v^2, b=3u^2+5uv-5v^2,$
$c=6u^2-4uv+4v^2, d=-5u^2+5uv$

がある（Ramanujan の恒等式）．さらに階数が 1 および 2 の各場合に，得られた生成元を利用して，C_m の整数点を決定する．

② ある条件を満たす合同数 N に伴う楕円曲

線 E^N についても，①と同様に，Silverman のアルゴリズムを使って標準的高さを精密に計算することにより，有理点群$E^N(\mathbb{Q})$の階数 2 または 3 の場合に$E^N(\mathbb{Q})$の生成元を決定する．

(2) ディオファンタスの 2 組$\{a,b\}$に対し，$\{a,b,c\}$ $(a<b<c)$ がディオファンタスの 3 組であるような最小の c の上限を b を使って表す．証明には連立有理数近似の改良および Baker-Davenport の還元法を利用する．

次に，a と b が非常に近いとき，$\{a,b,c\}$ がディオファンタスの 3 組となるような c を連立 Pell 方程式から得られる数列を使って明示的に表示する．これにより，$\{a,b\}$ のディオファンタスの 5 組への拡張可能性を調べることができる．

４．研究成果

(1)

① Fermat の 3 次式の 3 次 twist $C_m: x^3+y^3=m$ （m は 3 乗因子をもたない整数)について，まず，有理点群 $C_m(\mathbb{Q})$ の階数が 1 ならば C_m 上には高々2 つの整数点があり，それらのいずれもが $C_m(\mathbb{Q})$ を生成しうることを証明した．

さらに，$C_m(\mathbb{Q})$ の階数が2 ならば，C_m 上の任意の 2 つの整数点 P,Q $(P\neq \pm Q)$ は $C_m(\mathbb{Q})$ を生成し，しかもそのときC_m の整数点は高々$\pm P, \pm Q, \pm(P+R)$ の 6 点であることを示した．これらの結果は Acta Arithmetica より出版された．

② 合同数 N に伴う楕円曲線$E^N: y^2=x^3-N^2x$ について，E^N の有理点群 $E^N(\mathbb{Q})$ の階数が 2 や 3 以上となるような N の無限族を与え（例えば $N=3(2\alpha^2-\beta^2)(\alpha^2+\beta^2)(\alpha^2-2\beta^2)$ が平方因子をもたなければ階数は 2 以上であり，さらに $\alpha^2+\beta^2$ が平方数となる場合には階数は 3 以上である)，それらの場合に$E^N(\mathbb{Q})$ の生成元を完全に決定した．この結果は Journal of the Ramanujan Mathematical Society より出版された．

(2) $a<b<a+4\sqrt{a}$ や $b=4a\pm 4$ 等の様々なディオファンタスの 2 組$\{a,b\}$について，2 つの代数的数の対数の 1 次形式に関する Baker の方法と Rickert による連立有理数近似の改良，および Baker-Davenport の還元法を利用することにより，ディオファンタスの 5 組に拡張できないことが証明でき，それらの結果が Journal of Number Theory から出版された．

また，$b\leq 3a$ を満たす 2 組$\{a,b\}$については，Rickert の連立有理数近似をさらに改良することにより，ディオファンタスの 5 組に拡張できないことが証明でき，その結果は Glasnik Matematicki より出版された．

さらに，この結果を拡張し，a とb の最大公約数を g とするとき，$b\leq 3ga$ を満たすディオファンタスの 2 組$\{a,b\}$はディオファンタスの 5 組に拡張できないこと等を証明することができ，その結果は Publicationes Mathematicae Debrecen より出版された．

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７件）

① Mihai Cipu, Alan Filipin, Yasutsugu Fujita,
Bounds for Diophantine quintuples II, Publicationes Mathematicae Debrecen, 査読有, 88, 2016, pp.59-78
DOI: 10.5486/PMD.2016.7257

② Mihai Cipu, Alan Filipin, Yasutsugu Fujita,
Bounds for Diophantine quintuples, Glasnik Matematicki Series Ⅲ, 査読有, 50, 2015, pp.25-34
DOI: 10.3336/gm.50.1.03

③Yasutsugu Fujita, Tadahisa Nara, Generators and integral points on twists of the Fermat cubic, Acta Arithmetica, 査読有, 168, 2015, pp.1-16
DOI: 10.4064/aa168-1-1

④Alan Filipin, Yasutsugu Fujita, Alain Togbe,
The extendibility of Diophantine pairs II: examples, Journal of Number Theory, 査読有, 145, 2014, pp.604-631
DOI: 10.1016/j.jnt.2014.06.020

⑤Christian Elsholtz, Alan Filipin, Yasutsugu Fujita,
On Diophantine quintuples and D(-1)-quadruples, Monatshefte fur Mathematik, 査読有, 175, 2014, pp.227-239
DOI: 10.1007/s00605-013-0571-5

⑥Yasutsugu Fujita,
Generators for congruent number curves of ranks at least two and three, Journal of the Ramanujan Mathematical Society, 査読有, 29, 2014, pp.307-319
http://journals.thescientificindian.com/jrms/2010-19

⑦Yasutsugu Fujita, Takafumi Miyazaki,
Jeśmanowicz' Conjecture with Congruence Relations. II,
Canadian Mathematical Bulletin, 査読有, 57, 2014, 495-505

DOI: 10.4153/CMB-2014-020-0

〔学会発表〕（計４件）
①Yasutsugu Fujita,
Extendabilities of a Diophantine triple to quadruples, Analytic Number Theory and Related Areas, 2015/11/05, 京都大学数理解析研究所(京都府・京都市)

②Yasutsugu Fujita,
Bounds for Diophantine quintuples, Diophantine Analysis and Related Fields 2015, 2015/03/05, 桐生市民文化会館(群馬県・桐生市)

③Yasutsugu Fujita,
Diophantine quintuples: Bounds on the elements and the number, Conference on Diophantine m-tuples and related problems, 2014/11/13, Westville (USA)

④Yasutsugu Fujita,
Generators for twists of Fermat's cubic and congruent number curves, Diophantine analysis and related fields 2014, 2014/03/08, 筑波大学(茨城県・つくば市)

〔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
なし.

６．研究組織

(1)研究代表者
藤田　育嗣　（FUJITA, Yasutsugu）
日本大学・生産工学部・准教授
研究者番号：50514163

(2)研究分担者
寺井　伸浩（TERAI, Nobuhiro）
大分大学・工学部・教授
研究者番号：00236978
（平成 26 年度より研究分担者）

(3)研究協力者
奈良　忠央（NARA, Tadahisa）
東北学院大学・工学部・非常勤講師