HOKKAIDO UNIVERSITY

Title	Two researches on elliptic curves : the rank problem in cyclotomic towers of function fields and an application to integer factorization using the CM method [an abstract of dissertation and a summary of dissertation review]
Author(s)	相川, 勇輔
Degree Grantor	北海道大学
Degree Name	博士(理学)
Dissertation Number	甲第13551号
Issue Date	2019-03-25
Doc URL	https://hdl.handle.net/2115/74184
Rights(URL)	https://creativecommons.org/licenses/by-nc-sa/4.0/
Type	doctoral thesis
File Information	Yusuke_Aikawa_abstract.pdf, 論文内容の要旨

Hokkaido University Collection of Scholarly and Academic Papers : HUSCAP

学 位 論 文 内 容 の 要 旨

博士の専攻分野の名称　博士（理 学）　氏 名　相川　勇輔

学 位 論 文 題 名

Two researches on elliptic curves: the rank problem in cyclotomic towers of function fields and an application to integer factorization using the CM method

（ 楕円曲線に関する二つの研究: 関数体の円分拡大列におけるランク問題と素因数分解への CM 法を用いた応用）

本論文は楕円曲線に関する二つの独立した研究で構成される．以下でそれぞれの概要について述べる．

一つ目の研究テーマは関数体上の楕円曲線のディオファントス問題である．本論文で示される研究成果は，関数体上の楕円曲線の研究を行い，Mazur による予想 (1972) の関数体類似に対し新たな肯定的例を構成したことである．すなわち，関数体の円分拡大列に対して有界な階数を持つ楕円曲線を構成したことである．また，楕円曲線の階数の計算に超幾何関数のモノドロミーを応用するという手法の開発も本研究の重要な貢献である．以下において，本研究の背景および成果について詳しく述べる．

ディオファントス問題は，古来より研究されてきた整数論において重要な研究課題の一つである．それは，与えられた不定方程式の有理数上の，あるいはより広く数論的な体（代数体や有限体や局所体，関数体など）上の解を求める問題である．この問題は非常にシンプルで問題を理解するのは易しいが，例えばフェルマー予想のように，実際に解こうとすると極めて困難な場合がほとんどであり，依然として未解決問題が山積している．一方で楕円曲線は，3 次方程式で定義される代数曲線であり，整数論において極めて重要な研究対象である．こちらも簡明に定義される対象であるが，その数論的性質の多くは未だ謎に包まれている．本研究ではこの楕円曲線に対するディオファントス問題に取り組んだ．

楕円曲線の著しい性質はその解のなす集合が群構造を持つことである．従って楕円曲線のディオファントス問題はこの群構造を研究せよという問題であると言える．この研究の方向性において最も基本的かつ重要な定理が，代数体上の楕円曲線の解集合のなす群が有限生成アーベル群であることを主張する Mordell-Weil の定理である．この定理にちなんで楕円曲線の解集合はしばしば Mordell-Weil 群と呼ばれる．本研究の対象は関数体上の楕円曲線であるが，この場合でもその j-不変量が定数でないという条件の下，同様の定理が成り立つ．したがって，これらの体上の楕円曲線のディオファントス問題はその Modell-Weil 群の有限生成アーベル群としての階数とねじれ部分を計算せよという問題として定式化することができる．

さて，楕円曲線に関しては極めて多くの研究がなされてきた．ねじれ部分については決定的な研究が行われている一方で，その努力をもってしても階数については未だ我々は決定的な理解へ至っていない．例えば，有理数体上の楕円曲線のねじれ部分は Mazur により完全に分類されている一方で，階数

が有界かどうかさえわかっておらず，ミレニアム問題の一つである BSD 予想のような難題も提出されている．このように楕円曲線の階数は深淵な量であり，重要な研究対象であり続けている．

階数に対する予想の一つに Mazur によるものがある．それは $\mathbb{Z}_p$-拡大に対して Mordell-Weil 群が有限生成であるだろうというものである．整数論においては代数体と関数体の類似が古くから知られ，その両者を研究することによって互いの理解を深めてきた．それを踏襲し学位申請者は，Mazur 予想の関数体類似に取り組んだ．つまり，$\mathbb{C}(t)$ 上の楕円曲線 E に対し，$\mathbb{C}(t^{\frac{1}{n}})$ 上の Mordell-Weil 群 $E(\mathbb{C}(t^{\frac{1}{n}}))$ は n によらず有界であろうか？ という問いに取り組んだ．このように関数体上で考えると，塩田 (1990) の同型によって問題は楕円曲線 $E/\mathbb{C}(t)$ に対応する $\mathbb{P}^1$ 上の楕円曲面の Picard 数を求めるという幾何学的な問題へと移すことができる．

この問いに対しては，現状いくつかの肯定的例が構成されているのみである．それは Stiller(1987) や Fastenberg(1997) による．Stiller が提示した楕円曲線の例の中に，対応する楕円曲面が $\mathbb{P}^1$ 上の 2 点で乗法的退化をし，1 点で加法的退化するという性質を持つものがある．この退化する点を $\{0, 1, \infty\}$ とする．この対象を $\mathbb{P}^1 \to \mathbb{P}^1;\ t \mapsto \alpha - t\ (\alpha \in \mathbb{C} \setminus \{0, 1\})$ により底変換することで得られる楕円曲面の生成ファイバーとして得られる楕円曲線は，Stiller や Fastenberg が扱った対象とは本質的に異なり，彼らの手法だけでは階数の計算を実行できないことが本研究で明らかになった．本研究での学位申請者の貢献は，このようにして得られた楕円曲線の階数を計算を実行し，その帰結としてこれらが Mazur 予想の関数体類似を肯定する新たな例を与えることを明らかにしたことである．この階数計算の中で最も重要なステップは楕円曲面の 2 次のコホモロジーへのモノドロミー表現の計算を実行する部分であるが，その計算を朝倉-大坪 (2017) による結果を用いて楕円曲面の周期計算を通して超幾何関数のモノドロミーの計算に帰着させるという手法を開発したことも本研究の成果である．超幾何関数のモノドロミーは Beukers-Heckman(1989) の結果により計算可能であることから，この帰着によりコホモロジーへのモノドロミー表現が計算可能となり，その結果として階数計算が達成された．

二つ目の研究テーマは楕円曲線の素因数分解アルゴリズムへの応用である．本研究は縫田光司氏（東京大学）と白勢政明氏（公立はこだて未来大）との共同研究である．

素因数分解アルゴリズムは純粋に数学的関心から古来より研究されてきたが，現代においては RSA 暗号のような公開鍵暗号がその安全性の根拠に素因数分解問題の計算量的困難性をおくことから，その安全性評価の上でも研究の重要性が増している．一般の合成数に対する素因数分解アルゴリズムは準指数時間であるものしか現状知られていないが，例えば Pollard の $p-1$ 法のように特殊な素数に対しては効率的に働くようなアルゴリズムが知られている．

そのような中で本研究で我々は特殊な形をした素数を素因数に持つ合成数に対する多項式時間素因数分解アルゴリズムを提案する．本アルゴリズムは Lenstra Jr.(1987) による楕円曲線法と Atkin と Morain(1993) による特殊な位数を持つ楕円曲線生成法である CM 法を組み合わせたものとなっている．この研究の方向性については白勢 (2017) によってまず高速なアルゴリズムが提案された．それは素数 p が判別式 $-D$ を用いて $4p = 1 + Dv^2\ (v \in \mathbb{Z})$ と書ける場合，そのような素数を素因数に持つ合成数を高速に分解するものであるが，判別式の類多項式の次数が 2 次以下でなくてはならないという強い制約があった．

それに対して我々はその類多項式の次数に関する強い条件を外しアルゴリズムの一般化を行なった．さらに，先行研究では $4p = 1 + Dv^2$ という形の素数を扱っていたのに対し，より一般に $4p = t^2 + Dv^2$ という形をしていても $p + 1 - t$ がスムースとなる場合は適用できる形にアルゴリズムを拡張した．