



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_review.pdf, 審査の要旨



学 位 論 文 審 査 の 要 旨

博士の専攻分野の名称 博士 (理学) 氏 名 相川 勇輔

主 査 教 授 朝倉 政典
審査担当者 副 査 教 授 松本 圭司
 副 査 准教授 松下 大介

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)

博士学位論文審査等の結果について (報告)

近年、楕円曲線に関する研究が盛んに行われている。それは純粋数学のみならず、暗号理論をはじめとする応用数学としても重要な研究対象となっているからである。相川勇輔氏は、楕円曲線に関して、2つの重要な研究を行った。

ひとつは楕円曲線のディオファントス問題についての研究である。代数体上定義された楕円曲線の有理点の集合が有限生成アーベル群になることは Mordell-Weil の定理と呼ばれ、よく知られているが、そのランクについては、いまだ未解決の課題が多い。例えば、有理数体上の楕円曲線の場合は、そのランクが L 関数の $s=1$ における零点の位数になると予想されている。これは、Birch, Swinnerton-Dyer 予想と呼ばれ、クレイ研究所が提出した7つのミレニアム問題のひとつである。一方、Mazur (1972) は、基礎体を円分 $\mathbb{Z}_p$ 拡大体に取り換えても、ランクは有限になるだろうと予想した。この問題も、いまだ未解決である。

相川氏は、本学位論文において、基礎体を代数体ではなく、複素数上の1変数代数関数体にした場合に、Mazur の予想の類似を考え、この予想に対して肯定的かつ非自明な具体例を構成した。彼は、関数体上の楕円曲線を、複素代数曲線を基とする楕円ファイブレーションに取り換え、その Neron-Severi 群のランクの計算に帰着させた。こうして、複素幾何学の手法を適用できるようになる。ここで、彼が適用した理論は、ホッジ理論と超幾何関数である。一般的に言って、与えられた曲面の Neron-Severi 群を決定するのは、容易ではない。彼は、この困難を、ホッジ構造とモノドロミーのテクニックを使って克服した。その際、証明のキーになるのは、楕円曲面の周期積分が超幾何関数を用いて記述されるという事実である。彼はこの事実を使って、超幾何関数のモノドロミーの定理に帰着させることで、Neron-Severi 群のランクを完全に決定した。

相川氏は、本論文において、複素幾何学における強力な理論・道具を縦横に用いており、内容的に極めて水準が高い。また、本論文の主定理は、数論幾何学における重要なテーマである楕円曲線のランク問題に基づくものであって、結果そのものも、興味深く重要なものといえる。

相川氏が行ったもうひとつの研究は暗号理論に関するものである。現代の暗号システムでもっとも一般的に使用されているものが公開鍵暗号と呼ばれるものである。暗号は外部の者に解読されてはならず、安全性が保証されなければならない。公開鍵暗号の安全性は、数学における単純な事実、

すなわち、桁数の大きい整数の素因数分解は計算機を使っても困難である、という事実に基づいている。逆に言うと、素因数分解を高速で実行する手法ないしコンピューターが出現すれば、現代の暗号システムの大半が崩壊する。

暗号理論とは、高速で素因数分解を行う方法を理論的に追究していく理論である。つまり、高速で素因数分解できてしまうような整数の特徴を明らかにすることで、公開鍵暗号で使用するはならない整数、使用してよい整数を明らかにすることを目的としている。近年では、楕円曲線を用いた研究が盛んである。楕円曲線法とよばれる素因数分解の方法は、数十桁の整数の素因数分解を高速で行うことを可能にする。

本論文において、相川氏は、共同研究者とともに、この楕円曲線法を研究し、新しい素因数分解の方法を開発した。彼らが着目したのは、虚数乗法とよばれる整数論の理論である。この手法の開発によって、ある特徴をもつ整数(虚数乗法論によって特徴付けされる)については、従来の方法よりもはるかに高速で素因数分解ができるようになった。楕円曲線暗号における画期的な業績と言える。この研究においては、虚数乗法論という整数論が最も重要な役割を果たしているが、純粋数学的な議論は、相川氏が中心になって行った。この研究における彼の貢献は、非常に大きい。

以上の観点から、著者は、北海道大学博士(理学)の学位を授与される資格あるものと認める。