所属： 豊田工業高等専門学校　一般学科

研究タイトル：

与えられたコンダクターをもつ楕円曲線の決定

氏名：	筒石　奈央　／TAKESHI　Nao	E-mail：	takeshi @toyota-ct.ac.jp
職名：	助教	学位：	博士（理学）
所属学会・協会：	日本数学会		

キーワード：	楕円曲線，単数方程式
技術相談 提供可能技術：	

研究内容：

研究概要　代数体上の楕円曲線で、与えられたコンダクターを持つものの存在性を、単数方程式を用いて調べている。合わせて楕円曲線と保型形式との対応関係を見出すことも目指している。

背景　楕円曲線とは$y^2 = x^3 + ax + b$ $(4a^3 + 27b^2 \neq 0)$で定義された代数曲線のことであるが、これは、数論や幾何学、代数幾何学、複素関数論等、数学の様々な分野に登場する重要な研究対象である。例えば、いわゆるフェルマーの最終定理（1995，Wiles）に代表される古来考察されてきた多くの数論の問題が楕円曲線に帰着されることを見ても、楕円曲線研究の重要性がわかるだろう。

その楕円曲線でも、コンダクターが1の（つまり，全ての素イデアルでgood reductionをもつ）ものを最初に研究の対象にしたのはTate である。彼は有理数体Q上にはそのような楕円曲線は定義されないことを示した（1960 年頃）。この研究の背景にあるのは、志村-谷山予想である。これは、全く素性の異なる楕円曲線（数論的対象）と保型形式（解析的対象）とがうまく対応する、という予想である。Q上のコンダクターが1の楕円曲線と対応が予想されていたのは、レベルが1 の保型形式（重さ2）である。そのような保型形式は0しか存在しないことより、Tate は、志村-谷山予想が2001 年にWiles らによって解決される遥か昔に予想を部分的に解決したことになる。一般の代数体においても、対応が予想されており、解決に向けて研究が活発になされている。しかし、多少の進展はあるものの、その詳細は未だ不明なところが多い。そこで、一般化への足掛かりを得るためにも、小さいコンダクター（楕円曲線）とレベル（保型形式）をもつ両者それぞれを詳しく研究し、具体的な体で対応関係を見出すことを目指し、楕円曲線サイドからの研究を行っている。

対応関係を調べる第一歩は、与えられたコンダクターをもつ楕円曲線を決定し、isogeny classに分けることであるが、一般の代数体上でそのような楕円曲線を決定すること自体、容易ではない。これまで、コンダクター1の場合について多くの研究が行われており、特に2次体上の決定問題についての結果が多くある。しかし、判別式の小さい2次体ですら未決定の体があり、3次以上の体については、個別の体での結果があるのみであった。

研究内容　そこで私は、まず3次体上でコンダクター1をもつ楕円曲線について研究し、そのような楕円曲線が定義されないための十分条件を与えた。その鍵になったのが、単数方程式の解を用いて楕円曲線を構成する方法である。その方法を応用することで、「コンダクター1をもつ楕円曲線の無限族」、「任意の代数体Kと、任意の素イデアルの有限集合Sに対して、 K上定義される楕円曲線でSの外good reductionを持つもの(Sが空集合の時がコンダクター1)を決定するアルゴリズム」が得られている。また、Sが空集合の場合にアルゴリズムに沿った形でKを入力すると全ての楕円曲線を返すプログラムをMAGMA上に実装し、それを用いて新たな決定例が得られている。

しかしながら、現状のプログラムでは計算ができない代数体も多い。その原因として、現在単数方程式の計算はMAGMA のコマンドを用いているが、単数方程式が定義される体の単数群のランクが大きく計算許容範囲を超える場合があることが挙げられる。また、S が空集合でない場合のアルゴリズムは未実装である。

そこで、S が空集合でない場合に必要な S-単数方程式を解く過程も含めて、アルゴリズムを再構築したいと考えている。S-単数方程式の解法については Wildanger のアルゴリズム(2000)を元にするが、楕円曲線決定に必要な方程式に特化した形でアルゴリズムを構築し、それに沿った形でプログラムを MAGMA に実装したいと考えている。

提供可能な設備・機器：

名称・型番（メーカー）	