

令和 3 年 6 月 4 日現在

機関番号：12701

研究種目：基盤研究(C) (一般)

研究期間：2017～2020

課題番号：17K05196

研究課題名(和文) アーベル多様体のモジュライ空間や曲線のモジュライ空間の階層構造の研究

研究課題名(英文) Stratifications of the moduli space of abelian varieties and that of curves

研究代表者

原下 秀士 (Shushi, Harashita)

横浜国立大学・大学院環境情報研究院・准教授

研究者番号：70396852

交付決定額(研究期間全体)：(直接経費) 3,500,000円

研究成果の概要(和文)：本研究の扱う、アーベル多様体や代数曲線は数学の代数幾何学という分野において、中心的な役割を果たす研究対象であり、数学の他分野にも多くの応用を持つ。また、社会的にも、耐量子計算機暗号など次世代の情報技術にも用いられる対象(超特異曲線)があり、特にその部分について深い研究を行っている。研究成果としては、アーベル多様体や代数曲線等に付随する p -可除群という対象があるがその特殊化のタイプの決定や、低種数低標数の様々なタイプの超特別曲線の数え上げ(計算機を用いた結果)、一般の標数において種数4の超特別曲線の存在(理論的結果)などを行った。

研究成果の学術的意義や社会的意義

本研究では、アーベル多様体や代数曲線のモジュライ空間に入る階層構造や葉層構造を系統的に研究している。理論的研究と共に、応用面でも利用される超特異アーベル多様体や超特異代数曲線、またそれらのなす空間についても深く調査している。特に、超特異代数曲線やそれらの間の同種写像は、耐量子計算機暗号等にも用いられ、本研究が社会的に意義のある成果を生み出す可能性がある。

研究成果の概要(英文)：Abelian varieties and algebraic curves treated in this research play central roles in algebraic geometry of mathematics and have many applications in other areas. Socially, there are objects (supersingular curves) that will be used in next-generation information technology such as post-quantum cryptography, and we are intensely studying those objects. As research results, we determine specializations of p -divisible groups (which are attached to abelian varieties and algebraic curves) and enumerate superspecial curves (of various types) of low genera and in small characteristics (using PC computations), and show the existence of a superspecial curve of genus 4 in arbitrary characteristic (theoretical result) and so on.

研究分野：代数学

キーワード：代数幾何学 アーベル多様体 代数曲線 モジュライ空間 超特異

1. 研究開始当初の背景

アーベル多様体のモジュライ空間について、階層構造や葉層構造はそれぞれ、深く研究され個々の階層や葉層の基本的な構造(次元や既約成分)は良く分かってきている。ただ、その配置の様子や、特異点などその深い情報については未解決な問題が多く残されている。特に、葉層構造の配置は未だ決定されておらず、この分野の中心的な課題の一つである。また、アーベル多様体を曲線に変えた場合は、(散発的な結果はあるが)ほとんど分かっていない状況であった。先駆的な結果として、工藤氏との共同研究で、計算機的手法により、標数 7 以下の種数 4 の超特別曲線の数え上げを行い、特に標数 7 の種数 4 の超特別曲線が存在しない事を示し、その応用として、位数 49 の体上の種数 4 の曲線の有理点の個数の最大値を決定した。本研究は、その結果・手法の深化を目指したものである。種数 4 以上の超特異曲線や超特別曲線の理論的な存在・非存在の研究は少なく、何等かの breakthrough が期待されている状況であった。

2. 研究の目的

アーベル多様体のモジュライ空間は、代数幾何学の重要な研究対象であり、同時に保型形式論との関りから整数論等への多くの応用も持つ興味深い空間である。しかし、その基本構造において未解決問題が多く残されている。特に葉層構造については、その配置が依然不明であり解決が望まれている。また、曲線の場合はほとんど分かっていないため、超特別曲線の存在性や数え上げを様々な場合に計算機的手法で行い、存在性・非存在性・数え上げについて予想をたて、今後の理論的展開に貢献したい。もちろん可能であれば、理論的な成果をあげて行きたい。超特異曲線・超特別曲線は、その同種写像を用いて、耐量子計算機暗号等に用いられており、超特異・超特別曲線の存在性・非存在性の証明やその数え上げは、将来このような応用分野にも寄与すると考えている。同種写像は、暗号理論だけでなく、上記の数え上げ問題においても、高速なアルゴリズムの作成に寄与している。超特別の場合に詳しく調べられているが、他の場合には不明なところもあり、今後の研究の進展が期待されているところである。

3. 研究の方法

アーベル多様体のモジュライ空間において Newton polygon 階層は特に興味深く、その階層は central leaf と isogeny leaf による擬積構造を持つので、それぞれの leaf を深く調べることが重要である。まず、最も特徴的な central leaf である central stream の境界の Newton polygon の決定を行い、その後、前研究と合わせ、変形の詳しい解析を行うことにより、central leaf の境界の決定を行う。central stream とその他の central leaf の差を、同種のモジュライ空間でとらえ、一般の central leaf の境界の決定に挑む。曲線のモジュライ空間に対しては、超特別曲線が存在するか否かという問いに対して、種数 4 の場合の結果・手法(工藤氏との共同研究)を踏まえ、他の場合にも結果を積み上げていく。種数 4 の場合は、Howe による二つの楕円曲線の射影曲線上のファイバー積を用いた構成が知られており、その構成から曲線は良い性質を持つことが分かるので、この曲線を用いた理論的な成果(種数 4 の超特異曲線の存在性)を証明する。種数 5 以上になると、曲線のモジュライ空間が巨大になるため、なるべく(超楕円、gonality 等の概念を用い)曲線の範囲を狭め、その範囲での、超特異・超特別曲線の存在性・非存在性を論じ、可能であればその数え上げを行う。また曲線のモジュライ空間に対する Ekedahl-Oort 階層の研究に着手し、今後の研究の幅を広げる。

4. 研究成果

・アーベル多様体のモジュライの葉層構造については、2018 年の Nagoya Mathematical Journal の論文で、Newton polygon が saturated である p -可除群を、同種を用い、より単純なものに移す研究を行った。この結果は、様々な問題を、より単純なものの特殊化に帰着できる可能性を示唆しており、問題によってはより単純なもののみを考察すればよくなったので、非常に大きな進展であった。また、私の学生の樋口君が、minimal p -可除群の generic な特殊化の分類を行い、その Ekedahl-Oort タイプと Newton polygon の決定を完全に行った。解決に向けて大きな進展が得られたと考えている。両者を合わせて、葉層構造の境界の決定問題の解決に大きく近づいたと考えている。

・低標数、低種数の超特別曲線の数え上げについて、工藤氏と多くの論文を執筆した。特に、種数 4 の標準曲線について小さい標数や小さい体で超特別曲線の数え上げを行った。具体的には、標数 7 以下の体についての数え上げは行っていたので、標数が 11 以下の素体上の種数 4 の標準曲線で超特別なもの数え上げを行った(Tokyo Journal of Mathematics に採択)。超楕円の場合ももちろん調査しており、標数 19 以下の種数 4 の超特別超楕円曲線、標数 23 以下の素体上の種数 4 の超特別超楕円曲線の数え上げを、計算機的手法で行った。種数 5 については、超楕円だけでなく trigonal の場合の数え上げを行った。まず、trigonal 曲線を(定義体の情報を保ったまま)射影平面上の 5 次曲線(一つの特異点をもつ)もので実現し、その上の Hasse-Witt 行列の記述を与え、種数 5 の超特別 trigonal 曲線の数え上げのアルゴリズムを提案した。同論文

で、そのアルゴリズムの実装を行い、標数が7以下の種数5の超特別 trigonal 曲線、標数が13以下の素体上の種数5の超特別 trigonal 曲線の数え上げを行った。この trigonal 曲線の場合の論文は、Experimental Mathematics に採択された。種数5の曲線は、超楕円曲線、trigonal 曲線、4次元射影空間内の3つの2次曲線の交叉、の3種類であることが知られており、残されたこの第3のケースについて、最近論文を執筆した。3つの2次曲線の交叉で実現すると、パラメータの数が膨大で、数え上げについては絶望的であったが、その曲線上から2点を選び、射影平面に射影することにより、射影平面内の6次曲線で実現し、効率の良いパラメトリゼーションを与えることに成功した。もちろん定義体の情報は保っている。6次曲線は特異点を持っており (generic には5点の2重特異点である) 、その特異点の配置の決定、およびその位置に特異点をもつ6次曲線をパラメトライズすることにより、数え上げが可能になった。ただし、まだまだ巨大な空間のため、定義体は位数3の体で、実装したアルゴリズムの実行をおこなった。また、5つの2重特異点以外に、1つの3重点と2つの2重点の場合もあり、その場合も実行を行っている。本論文は arXiv に投稿し、MEGA 2021 のプレゼンテーション論文に採択された。ただ、他にも悪い特異点を持つ場合があり、それは今後の課題としている。

・また、理論的結果として、種数4において任意の標数で超特異曲線の存在を証明することが出来た。長い歴史がある分野だが、昔からある未解決問題であったため、私自身も驚くような成果となった。これは、工藤氏、私の学生の千田君との共同研究であり、学術雑誌 Research in Number Theory に採択された。また、この証明で用いた曲線で超特別なものの計算機的な数え上げについて、工藤氏、E. Howe 氏と共同研究を行った。超高速な、種数4の超特別曲線の発見・数え上げアルゴリズムを得ることができた。そのアルゴリズムの実装・実行により、20000以下の標数に対し、種数4の超特別曲線の存在を証明した。また、標数199以下においては、種数4の超特別 Howe 曲線の同型類の数え上げも行うことができた。この論文は、14th ANTS のプレゼンテーション論文に採択された。工藤氏と千田氏とは、種数4の非超楕円曲線の自己同型群を求めるアルゴリズムの提出と、標数11における自己同型群の決定の論文も執筆し、その論文は Journal of Pure and Applied Algebra に採択された。

5. 主な発表論文等

〔雑誌論文〕 計9件（うち査読付論文 8件 / うち国際共著 1件 / うちオープンアクセス 2件）

1. 著者名 Kudo Momonari, Harashita Shushi, Senda Hayato	4. 巻 224
2. 論文標題 Automorphism groups of superspecial curves of genus 4 over F_{11}	5. 発行年 2020年
3. 雑誌名 Journal of Pure and Applied Algebra	6. 最初と最後の頁 106339 ~ 106339
掲載論文のDOI (デジタルオブジェクト識別子) 10.1016/j.jpaa.2020.106339	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 -
1. 著者名 Kudo Momonari, Harashita Shushi	4. 巻 0
2. 論文標題 Superspecial Trigonal Curves of Genus 5	5. 発行年 2020年
3. 雑誌名 Experimental Mathematics	6. 最初と最後の頁 1 ~ 12
掲載論文のDOI (デジタルオブジェクト識別子) 10.1080/10586458.2020.1723745	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 -
1. 著者名 Harashita Shushi	4. 巻 297
2. 論文標題 Asymptotic formula of the number of Newton polygons	5. 発行年 2020年
3. 雑誌名 Mathematische Zeitschrift	6. 最初と最後の頁 113 ~ 132
掲載論文のDOI (デジタルオブジェクト識別子) 10.1007/s00209-020-02504-w	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 -
1. 著者名 Nobuhiro Higuchi and Shushi Harashita	4. 巻 64
2. 論文標題 On specializations of minimal p -divisible groups	5. 発行年 2018年
3. 雑誌名 Yokohama Mathematical Journal	6. 最初と最後の頁 1 ~ 20
掲載論文のDOI (デジタルオブジェクト識別子) なし	査読の有無 有
オープンアクセス オープンアクセスとしている (また、その予定である)	国際共著 -

1. 著者名 Momonari Kudo and Shushi Harashita	4. 巻 11321
2. 論文標題 Superspecial hyperelliptic curves of genus 4 over small finite fields	5. 発行年 2018年
3. 雑誌名 Lecture Notes in Computer Science	6. 最初と最後の頁 58 ~ 73
掲載論文のDOI (デジタルオブジェクト識別子) なし	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 -

1. 著者名 Kudo Momonari, Harashita Shushi	4. 巻 45
2. 論文標題 Superspecial curves of genus 4 in small characteristic	5. 発行年 2017年
3. 雑誌名 Finite Fields and Their Applications	6. 最初と最後の頁 131 ~ 169
掲載論文のDOI (デジタルオブジェクト識別子) 10.1016/j.ffa.2016.12.001	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 -

1. 著者名 HARASHITA SHUSHI	4. 巻 232
2. 論文標題 ON p-DIVISIBLE GROUPS WITH SATURATED NEWTON POLYGONS	5. 発行年 2018年
3. 雑誌名 Nagoya Mathematical Journal	6. 最初と最後の頁 96 ~ 120
掲載論文のDOI (デジタルオブジェクト識別子) 10.1017/nmj.2017.22	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 -

1. 著者名 Kudo Momonari, Harashita Shushi, Howe Everett W.	4. 巻 4
2. 論文標題 Algorithms to enumerate superspecial Howe curves of genus 4	5. 発行年 2020年
3. 雑誌名 Open Book Series	6. 最初と最後の頁 301 ~ 316
掲載論文のDOI (デジタルオブジェクト識別子) 10.2140/obs.2020.4.301	査読の有無 有
オープンアクセス オープンアクセスとしている (また、その予定である)	国際共著 該当する

1. 著者名 Kudo Momonari, Harashita Shushi, Senda Hayato	4. 巻 6
2. 論文標題 The existence of supersingular curves of genus 4 in arbitrary characteristic	5. 発行年 2020年
3. 雑誌名 Research in Number Theory	6. 最初と最後の頁 Article no. 44
掲載論文のDOI (デジタルオブジェクト識別子) 10.1007/s40993-020-00217-x	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 -

〔学会発表〕 計8件 (うち招待講演 4件 / うち国際学会 5件)

1. 発表者名 Shushi Harashita
2. 発表標題 The existence of supersingular curves of genus 4 in arbitrary characteristic
3. 学会等名 Supersingular Abelian Varieties and Related Arithmetic (招待講演) (国際学会)
4. 発表年 2019年

1. 発表者名 Momonari Kudo (登壇者) and Shushi Harashita
2. 発表標題 Superspecial Hyperelliptic Curves of Genus 4 over Small Finite Fields
3. 学会等名 International Workshop on the Arithmetic of Finite Fields (WAIFI 2018) (招待講演) (国際学会)
4. 発表年 2018年

1. 発表者名 工藤桃成 (登壇者)、原下秀士
2. 発表標題 Superspecial trigonal curves of genus 5
3. 学会等名 日本数学会 (年会)
4. 発表年 2019年

1. 発表者名 Momonari Kudo and Shushi Harashita
2. 発表標題 Superspecial trigonal curves of genus 5
3. 学会等名 MEGA2019、ポスター発表（国際学会）
4. 発表年 2019年

1. 発表者名 Momonari Kudo (登壇者), Shushi Harashita
2. 発表標題 Enumerating Superspecial Curves of Genus 4 over Prime Fields
3. 学会等名 The Tenth International Workshop on Coding and Cryptography 2017 (招待講演) (国際学会)
4. 発表年 2017年

1. 発表者名 工藤桃成 (登壇者), 原下秀士
2. 発表標題 Enumerating superspecial curves of genus 4 over prime fields
3. 学会等名 日本数学会年会
4. 発表年 2018年

1. 発表者名 千田駿人 (登壇者), 工藤桃成, 原下秀士
2. 発表標題 Automorphism groups of superspecial curves of genus 4 over F_{11}
3. 学会等名 日本数学会年会
4. 発表年 2018年

1. 発表者名 Shushi Harashita
2. 発表標題 Supersingular abelian varieties and curves, and their moduli spaces
3. 学会等名 Theory and Applications of Supersingular Curves and Supersingular Abelian Varieties (招待講演) (国際学会)
4. 発表年 2020年

〔図書〕 計0件

〔産業財産権〕

〔その他〕

-

6. 研究組織

氏名 (ローマ字氏名) (研究者番号)	所属研究機関・部局・職 (機関番号)	備考

7. 科研費を使用して開催した国際研究集会

〔国際研究集会〕 計1件

国際研究集会 Theory and Applications of Supersingular Curves and Supersingular Abelian Varieties	開催年 2020年～2020年

8. 本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関