様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　２ 年　 ４ 月 ２３ 日現在

機関番号：５４５０２
研究種目：研究活動スタート支援
研究期間：2018～2019
課題番号：１８Ｈ０５８３６・１９Ｋ２１０２６

研究課題名（和文）計算代数手法による正標数の特殊な代数曲線に関する研究

研究課題名（英文）Study on special algebraic curves over fields of positive characteristic via computer algebra

研究代表者
工藤　桃成（Kudo, Momonari）

神戸市立工業高等専門学校・その他部局等・講師

研究者番号：１０８２４７０８

交付決定額（研究期間全体）：（直接経費）　　2,300,000円

研究成果の概要（和文）：代数曲線は主に代数幾何学・整数論の分野で古くから研究されている図形であり，暗号・符号理論などを含む情報通信分野への応用可能性が期待されている．
本研究では，そのような曲線の中でも超特別曲線・最大曲線に関する幾つかの問題に対し，理論と計算の融合的なアプローチによる研究を行い，解決に至った．特に，種数や標数と呼ばれるパラメータを具体的に決めたとき，これらの曲線の存在・非存在を明らかにすると共に，存在する場合にこれらの曲線をすべて求めることに成功した．
また，本研究の暗号理論への応用として，超特別（超特異）楕円曲線間の同種写像を高速に計算する手法を開発し，同種写像を利用した暗号の安全性評価にも貢献した．

研究成果の学術的意義や社会的意義
本研究では，超特別曲線・最大曲線と呼ばれる代数曲線について，種数と呼ばれるパラメータを固定したときに，上記曲線の存在・非存在性や数え上げに関する幾つかの問題の解決に取り組んだ．
本研究とその成果の学術的意義としては，先行研究では種数3以下の場合に多くの結果が得られていたのに対し，本研究では，これまで困難とされてきた種数4以上の場合を主に考察し結果が得られたという点で新規性が非常に高い．また，本研究では計算代数の手法を駆使している点で独自性が高い．
社会的意義としては，本研究で得られた曲線は暗号・符号理論において具体パラメータとして活用されうるという点で，情報通信分野などへの応用価値が期待される．

研究成果の概要（英文）：Algebraic curves are central objects studied in algebraic geometry, number theory and related areas, and they are expected to be applied to information technology, in particular, cryptography and coding theory.
In this study, we focused on algebraic curves said to be superspecial or maximal, and studied them by the combined approach of the theory of algebraic geometry and computer algebra. As a result, we have succeeded in solving several problems on the (non-)existence of superspecial curves and maximal curves, and problems on the enumeration of these curves.
Furthermore, as an application to cryptography, we proposed efficient algorithms to compute isogenies between superspecial (supersingular) elliptic curves. Developing these algorithms shall contribute to evaluate the security of the state-of-art isogeny-based cryptosystems.

研究分野：代数学

キーワード：代数幾何学　計算代数幾何　代数曲線　超特別曲線　最大曲線　正標数　Hasse-Witt行列　フロベニウス射

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

数学とその応用分野において，曲線は古くから研究されてきた重要な研究対象である．その中でも代数曲線（楕円曲線，超楕円曲線，etc.）とは，1 次元の代数多様体のことであり，主に代数幾何学や整数論において活発に研究されている．特に，正標数の体（e.g. 有限体）上の代数曲線は，暗号理論や符号理論などへの応用可能性を持つことで注目されている．

代数曲線の研究では，種数と呼ばれる最も基本的な離散不変量を固定したときに，与えられた値を不変量に持つ代数曲線の（非）存在性などを解明することが一つの目標となる．特に，正標数の体上では，「コホモロジー群上のフロベニウス写像の階数が 0」という不変量を持つ曲線は超特別曲線と呼ばれ，曲線のモジュライ空間全体の構造をより深く調べることができるなど，代数曲線の性質を分類する上で中心的な役割を果たす．それだけでなく，符号理論で重要な最大曲線などの他の特殊な曲線の（非）存在性や構造をも決定することが可能となる．このため，超特別曲線の（非）存在性を決定し，存在する場合その同型類をすべて決定することは，基本的であるが非常に重要な問題である．

曲線の種数が 3 以下の場合は，アーベル多様体の理論的手法などによって，任意標数に対し超特別曲線の（非）存在性・数え上げに関する結果が既に得られている（cf. 伊吹山氏，桂氏，橋本氏らによる先行研究）．一方で種数が 4 以上の場合は，種数が 3 以下の場合における上記手法が同様には機能しないと考えられており，存在性と数え上げに関する多くの未解決問題が残されている．特に，同型類の数え上げについては，種数 4，5 における小さい標数（p=11 など）の場合でさえ未解決であり，解決のためには種数 3 以下の場合における従来型の研究手法とは異なる新たなアプローチが必要となる．

２．研究の目的

本研究の目的は，代数曲線・アーベル多様体を分類する上で重要な役割を果たす超特別曲線・最大曲線と呼ばれる特殊な代数曲線について，計算代数幾何学の観点から深く研究を行うことで，これらの曲線の（非）存在性，数え上げ，さらには構造決定に関する幾つかの問題を解決することである．特に，これまで困難とされてきた，曲線の種数が 4 以上の場合における上記問題の解決に取り組む．また本研究では，学術論文の公開に加えて，得られる結果をデータベースとして一般公開するとともに，実装アルゴリズム・ソースコードを公開する．これにより，計算機の専門・非専門に関わらず，本研究に関係する分野の研究者に必要となるデータを容易に利活用出来るような環境を整備する．

３．研究の方法

本研究の方法として，①代数幾何学における理論的アプローチ，②計算代数におけるアルゴリズムと数式処理のアプローチ，の二つを融合させることで，上記目的の達成を目指す．以下で①，②を具体的に述べる．

① 超特別曲線の決定問題を何らかの計算問題に帰着させる．これにより，下記②のアプローチが有効となる．また，②において計算機を用いて得られた結果に関しては，再証明や他の理論結果（モジュライ空間の理論等）との整合性の確認を行う．

② グレブナー基底などの計算代数手法をもとに，上記①で帰着した計算問題を実時間で解くアルゴリズムを開発する．これにより，小さい標数 p に関しては，構成したアルゴリズムを計算機上で実行することで超特別曲線を決定できる見通しである．さらに，具体的な p に対して得られる結果と，その計算過程をもとに，一般的な結果を予想し，これを証明する．

４．研究成果

本研究の実施期間で得られた研究成果としては，以下の(1)～(7)である．

まず(1)は，超特別曲線と最大曲線の存在性に関するものである．

(1) ある合同式を満たす全ての素数 p に対して，標数 p の完全体上の超特別曲線（および素体 F_p の二次拡大体上の最大曲線）が存在することを示すと共に，そのような曲線の明示的な方程式を与えることにも成功した．特に，種数 4，5 の場合に上記の曲線が存在するような素数の密度はそれぞれ 1/2，1/4 であることを明らかにした．これらの結果をまとめた論文は，2019 年 3 月に国際雑誌 Communications in Algebra に掲載が受理された．

次の(2)は，超特別性の判定に用いる Hasse-Witt 行列の計算に関するものである．これは「３．研究の方法」②として開発したアルゴリズムの一部であるが，この研究方法（アルゴリズム）自体新しいものであり，本研究目的達成のために必須となるため，重要な結果として紹介する．

(2) Hasse-Witt 行列（コホモロジー群上のフロベニウス写像を表す行列）の計算の枠組みを大きく進展させた．具体的には，既存結果では特定の曲線（超楕円など）のみに計算手法が確立されていたが，本研究では一般次元の代数多様体への拡張に成功し，特に完全交叉（種数 4，5 の非超楕円曲線など）の場合に高速なアルゴリズムを開発した．この結果は 2019 年 6 月の査読付き国際会議 MEGA2019 に論文が採択され，現在その full paper を国際雑誌に投稿中である．また，本結果に対し日本数式処理学会若手研究者賞の受賞が決定している．

超特別曲線の数え上げに関して，原下秀士氏（横浜国立大学）と共同で(3)，(4)の結果を得た．

(3) 種数 4 の超楕円曲線の場合に，超特別曲線の数え上げ問題を計算問題に帰着させ，グレブナー基底などの計算代数手法を駆使することで，計算問題を解くためのアルゴリズムを提案した．アルゴリズムを計算機に実装・実行することで，標数 19 以下の任意有限体上，および標数 23 では素体の奇数次拡大体上で，超特別曲線を全て決定することに成功した．これらの結果をまとめた論文は査読付き国際会議 WAIFI2018 に採択されており，2018 年 12 月に予稿集 Lecture Notes in Computer Sciences 11321 に掲載された．現在その full paper を国際雑誌に投稿中である．

(4) 種数 5 の場合にも，トリゴナルと呼ばれる曲線クラスについて，方程式の記述と簡約化，および Hasse-Witt 行列の明示的公式などを与え，超特別曲線の小標数での数え上げに成功した．この結果について，査読付き国際会議 MEGA2019 にポスター発表が採択され，結果をまとめた論文が 2020 年 1 月に国際雑誌 Experimental Mathematics に掲載が受理された．

また，原下氏とその学生の千田駿人氏との共同研究で，次の(5)，(6)の結果を得た．

(5) 種数 4 の非超楕円曲線の自己同型群を計算するアルゴリズムを提案した．標数 11 の場合に超特別曲線の自己同型群を計算し，その群構造の決定に成功した．結果をまとめた論文は 2019 年 12 月に国際雑誌 Journal of Pure and Applied Algebra に掲載が受理された．

(6) 超特別曲線と関係の深い超特異曲線と呼ばれる曲線について，種数 4 の場合に任意標数での存在性を示した．この結果は国内外において高く評価され，2019 年 10 月に国際研究集会 Supersingular Abelian Varieties and Related Arithmetic にて依頼講演を行った．結果をまとめた論文を国際雑誌に投稿中である．

上記(2)～(5)で開発したアルゴリズムの実行プログラムは，報告者の web ページに公開しており，ダウンロード可能である．また，(3)，(4)で得られた超特別曲線・最大曲線，および(5)で計算した自己同型群についても，報告者の web ページ上にデータベースとして公開している．

さらに，安田雅哉氏（九州大学）らとの共同研究では，超特別曲線の暗号分野への応用として，同種写像暗号に関する(7)の結果を得た．

(7) 超特別（超特異）楕円曲線間の同種写像を高速に計算するアルゴリズムを開発し，結果をまとめた論文が，2019 年 8 月に査読付き国際会議 MathCrypt 2019 に発表が受理された．近年，同種写像を利用した暗号方式が多く提案されているが，本アルゴリズムを用いた暗号解読が可能である．本共同研究では解読によって暗号が脆弱となるパラメータをも明らかにし，同種写像暗号の安全性評価に貢献した．

５．主な発表論文等

〔雑誌論文〕　計4件（うち査読付論文　4件／うち国際共著　0件／うちオープンアクセス　0件）

１．著者名 Kudo Momonari、Harashita Shushi	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 L. Budaghyan, F. Rodriguez-Henriquez (eds), Arithmetic of Finite Fields, WAIFI 2018, 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） 10.1007/978-3-030-05153-2_3	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	４．巻 47
２．論文標題 On the existence of superspecial and maximal nonhyperelliptic curves of genera four and five	５．発行年 2019年
３．雑誌名 Communications in Algebra	６．最初と最後の頁 5020～5038
掲載論文のDOI（デジタルオブジェクト識別子） 10.1080/00927872.2019.1609013	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、Senda Hayato	４．巻 224 (9)
２．論文標題 Automorphism groups of superspecial curves of genus 4 over F11	５．発行年 2020年
３．雑誌名 Journal of Pure and Applied Algebra	６．最初と最後の頁 －
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 －
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 －
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 －

〔学会発表〕　計11件（うち招待講演　4件／うち国際学会　4件）

１．発表者名
工藤桃成、原下秀士

２．発表標題
Superspecial Trigonal Curves of Genus 5

３．学会等名
日本応用数理学会2018年年会「数論アルゴリズムとその応用」(JANT) セッション

４．発表年
2018年

１．発表者名
工藤桃成

２．発表標題
Superspecial curves of genera four and five

３．学会等名
第6回代数幾何学研究集会-宇部-（招待講演）

４．発表年
2019年

１．発表者名
工藤桃成、原下秀士

２．発表標題
Superspecial trigonal curves of genus five

３．学会等名
日本数学会2019年年会

４．発表年
2019年

１．発表者名
工藤桃成

２．発表標題
代数多様体のコホモロジー群へのフロベニウス作用を計算するアルゴリズム

３．学会等名
日本数式処理学会第28回大会

４．発表年
2019年

１．発表者名
Kudo Momonari

２．発表標題
Computing representation matrices for the Frobenius on cohomology groups

３．学会等名
Effective Methods in Algebraic Geometry (MEGA2019)（国際学会）

４．発表年
2019年

１．発表者名
Kudo Momonari, Harashita Shushi

２．発表標題
Superspecial trigonal curves of genus 5

３．学会等名
Poster Session at Effective Methods in Algebraic Geometry (MEGA2019)（国際学会）

４．発表年
2019年

１．発表者名
工藤桃成

２．発表標題
同種写像計算問題に対する代数的求解法の解析と計算量評価

３．学会等名
九州大学マス・フォア・インダストリ研究所暗号学セミナー（招待講演）

４．発表年
2019年

１．発表者名
工藤桃成

２．発表標題
暗号応用に向けた正標数代数曲線の存在性と数え上げ

３．学会等名
東京大学暗号数理セミナー（招待講演）

４．発表年
2019年

１．発表者名
Yasushi Takahashi, Momonari Kudo, Yasuhiko Ikematsu, Masaya Yasuda, Kazuhiro Yokoyama

２．発表標題
Algebraic approaches for solving isogeny problems of prime power degrees

３．学会等名
MathCrypt 2019（国際学会）

４．発表年
2019年

１．発表者名
高橋康、工藤桃成、池松泰彦、安田雅哉、横山和弘

２．発表標題
同種写像問題に対する代数的求解法の解析と計算量評価

３．学会等名
日本応用数理学会2019年年会「数論アルゴリズムとその応用」(JANT) セッション

４．発表年
2019年

１．発表者名
Kudo Momonari

２．発表標題
Computational approaches to superspecial curves of genera 4 and 5 over finite fields

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

〔図書〕　計0件

〔産業財産権〕

〔その他〕
ホームページ等
https://sites.google.com/view/m-kudo-official-website/home

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