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

平成　２９　年　　５　月　１０　日現在

機関番号：　２２６０４
研究種目：　若手研究(B)
研究期間：　2013～2016
課題番号：　２５８０００２３

研究課題名（和文）代数曲線とアーベル多様体に関する数論アルゴリズムの研究

研究課題名（英文）A study of algorithms on the arithmetic of algebraic curves and Abelian varieties

研究代表者

内田　幸寛（UCHIDA, Yukihiro）

首都大学東京・理工学研究科・准教授

研究者番号：９０５３３２５８

交付決定額（研究期間全体）：（直接経費）　　2,400,000円

研究成果の概要（和文）：代数曲線およびアーベル多様体の数論は理論と応用両方で非常に重要な主題である．代数体上あるいは有限体上定義された代数曲線およびアーベル多様体の数論に関するアルゴリズムとその応用について研究を行った．暗号用の計算困難問題，ある暗号方式への攻撃法，ヤコビ多様体上の高さの計算，楕円曲線上の秘密分散，Waringの問題に関係する不定方程式，種数2の曲線の位数計算に関する結果を得た．

研究成果の概要（英文）：The arithmetic of algebraic curves and Abelian varieties is a very important subject in both theory and applications. We studied algorithms and their applications on the arithmetic of algebraic curves and Abelian varieties defined over a number field or a finite field. We obtained results on computationally hard problems for cryptography, attacks against a certain cryptosystem, computation of heights on Jacobian varieties, secret sharing using elliptic curves, Diophantine equations related to Waring's problem, and counting points on curves of genus 2.

研究分野：　数論幾何学

キーワード：　アーベル多様体　ヤコビ多様体　高さ関数　楕円曲線　超楕円曲線　暗号

１．研究開始当初の背景

(1) 代数体上定義された代数曲線やアーベル多様体の有理点・整数点を決定する問題は，古くから研究されてきた不定方程式を解く問題と密接に関連し，数論において重要な問題である．20 世紀以降の代数幾何学の発展により，不定方程式を解く問題を，代数体上定義された代数曲線の整数点や有理点を求める問題に帰着して研究することで，大きな成果が得られてきた．これは現在数論幾何学と呼ばれる分野の重要なテーマの一つである．代数曲線は，種数と呼ばれる，非負整数値を取る不変量で分類される．種数１の代数曲線には，群構造が定義され，楕円曲線と呼ばれる．また，代数曲線から定まる，ヤコビ多様体と呼ばれる代数多様体を考えることで，もとの曲線の有理点の情報が得られることもある．楕円曲線やヤコビ多様体は，アーベル多様体と呼ばれる，群構造を持つ代数多様体の一種であり，より一般にアーベル多様体の有理点が研究されている．代数体上定義されたアーベル多様体の有理点は，有限生成アーベル群をなす（Mordell-Weil の定理）．この群を Mordell-Weil 群と呼ぶ．Mordell-Weil の生成元を決定するアルゴリズムは一般には得られていないが，具体的な対象については生成元が決定できることも多い．また，代数曲線のヤコビ多様体の Mordell-Weil 群を考えることで，もとの曲線の有理点が決定できる場合もある．これらのアルゴリズムについて，適用できる対象を増やし，また高速化を行うことは，不定方程式の解法という観点からも重要な課題である．

(2) 近年の暗号理論においては，代数曲線暗号やペアリング暗号に見られるように，有限体上定義された代数曲線やアーベル多様体の数論が暗号方式の構成に重要な役割を果たしている．有限体の乗法群に対する離散対数問題の代わりに，有限体上定義された楕円曲線やアーベル多様体の有理点がなす群に対する離散対数問題を考えることで，代数曲線暗号が構成される．また，代数曲線上定義された Weil ペアリングや Tate-Lichtenbaum ペアリングを利用することで，ペアリング暗号と呼ばれる新しい暗号方式が開発されてきている．これらのことから，有限体上定義された代数曲線やアーベル多様体の数論，およびそれに関連するアルゴリズムの研究は重要な課題である．

２．研究の目的

代数体上あるいは有限体上定義された代数曲線およびアーベル多様体に関する数論アルゴリズムを発展させ，有理点・整数点の決定や暗号理論への応用に役立てることを本研究の目的とする．

３．研究の方法

(1) 代数体上の代数曲線およびアーベル多様体に関する数論アルゴリズムの研究を行う．アーベル多様体上の標準高さの計算アルゴリズムの開発を行い，計算の高速化を目指す．また，これらのアルゴリズムを用いて具体的な曲線の有理点の決定を行う．

(2) 有限体上の代数曲線およびアーベル多様体に関する数論アルゴリズムの研究を行う．楕円曲線の等分多項式やその一般化である elliptic net について，超楕円曲線のヤコビ多様体への拡張がされているが，より一般のアーベル多様体に対する拡張の可能性も含めた研究を行う．また，これらの応用として，アーベル多様体の位数計算などのアルゴリズムの構成を行う．

４．研究成果

(1) Elliptic divisibility sequence (EDS) に対する計算困難な問題と楕円曲線上の Diffie-Hellman 問題について考察した．EDS とは，1948 年に M. Ward が定義した数列であり，楕円曲線の等分多項式の値がなす数列で，非線形な漸化式を満たしている．2008 年，Lauter と Stange は EDS に関するいくつかの計算困難な問題を定義し，それらと楕円曲線上の離散対数問題(ECDLP)が計算量的に等価であることを示した．本研究では，鑓水淳一氏，内山成憲氏との共同研究により，EDS に対する Diffie-Hellman 問題の類似物を定義し，楕円曲線上の Diffie-Hellman 問題と計算量的に等価であることを示した（雑誌論文③）．

(2) ディクソン多項式を用いた暗号方式に関して，秘密鍵が小さいときの攻撃法を考察した．ディクソン多項式を用いた暗号方式は，RSA 暗号や LUC 暗号の拡張にあたるものである．RSA 暗号には秘密鍵が小さいときの攻撃法として，連分数を用いるものや LLL アルゴリズムを用いるものが知られている．本研究では，尾西昭彦氏，内山成憲氏との共同研究により，ディクソン多項式を用いた暗号方式にこれらの攻撃法を適用し，RSA 暗号の場合と同様の攻撃法が適用できることを確かめた（学会発表⑥，雑誌論文②）．

(3) 超楕円ヤコビ多様体の標準高さの計算について，計算速度を向上するアルゴリズムの構成を行った．超楕円曲線のヤコビ多様体上の標準高さを計算するアルゴリズムについては，種数１（楕円曲線）の場合は高速なものが知られており，種数２の場合も計算が可能であった．最近になって，種数３以上を含む一般の場合に適用可能な，Arakelov 交点理論を用いる新しいアルゴリズムが，J. S. Müller，D. Holmes によって独立に提案された．どちらのアルゴリズムも，標準高さを Arakelov 交点数として表し，交点数を素点ごとの局所交点数に分解して計算する．このとき，無限素点での計算はテータ関数の計算に

帰着されるが，その数値計算は種数が大きいとき多大な計算時間を要する．本研究では，無限素点での計算を，テータ関数ではなく，Riemann面上でのAbel積分の計算に置き換えることで，高速化ができるかどうか調べた．その結果，種数が大きい場合には，大幅な計算時間の改善が見られるという実験結果を得た（学会発表④）．有限素点での寄与も含めた標準高さ全体の計算アルゴリズムについて，現在も検討を進めている．

(4) 楕円曲線を用いた秘密分散に関する研究を行った．秘密分散とは，秘密情報から構成したいくつかの分散情報を参加者に分散し，一部の参加者の分散情報を集めることで，もとの秘密情報を復元する方式である．1979年 Shamir と Blakley は独立に秘密分散方式を提案した．Shamir の秘密分散方式は多項式の補間公式を用いて秘密情報を復元するものである．通常の秘密分散では１個の秘密情報を分散するが，複数の秘密情報を一度に分散する秘密分散方式がこれまでに提案されている．また，秘密情報を楕円曲線の点として埋め込むことで秘密情報，分散情報を扱う方式も提案されている．本研究では，池田崇氏，内山成憲氏との共同研究において，これらを組み合わせて，複数の秘密情報を同時に，楕円曲線を用いて分散する方式を提案した（学会発表③）．

(5) Waring の問題や数値積分公式に関係する不定方程式系について，澤正憲氏との共同研究を行った．直交多項式の理論に基づいて定積分の近似値を求める Gauss 型数値積分公式を考える．この公式に現れる分点や重みは一般には無理数になるが，近似が悪くなることを許して分点と重みを有理数にする問題を考える．この問題は，Waring の問題に現れる Hilbert の恒等式とも関係する．この問題は，分点と重みを変数とする不定方程式系を有理数の範囲で解く問題と見なせるが，一方で，準直交多項式の零点すべてが有理数になるか判定する問題にも帰着される．この問題について，ある条件の下で有理数の分点と重みが存在しないことを，楕円曲線や超楕円曲線の有理点の問題に帰着することで証明した（学会発表②）．本研究はさらにより多くの条件下で結果を得ることを目指して現在も進行中である．

(6) 有限体上定義された種数 2 の曲線の位数計算について研究を行った．代数曲線暗号において，暗号に用いる曲線の位数を高速に計算することが重要な課題の一つである．位数計算アルゴリズムには，有限体の標数が小さいとき有効なものと，標数が大きいとき有効なものがあるが，ここでは標数が大きいとき有効なアルゴリズムを考察する．有限体の標数が大きい場合のアルゴリズムとして，いくつかの小さい素数 l に対して，代数曲線のヤコビ多様体の l 等分点がなす群を考え，その群へのフロベニウス写像の作用を用いる方法がある．この方法は楕円曲線や，種数 2 の超楕円曲線で虚モデルを持つ（超楕円曲線が有理的なワイエルシュトラス点を持つ）場合には実装されていたが，それ以外の場合には理論的な結果しかなかった．本研究では，種数 2 の超楕円曲線で実モデルを持つ場合について，位数計算アルゴリズムの実装に向けて研究を行った．その結果，研究代表者が以前に得ていたクンマー曲面上の乗法公式を用いることで位数計算アルゴリズムが構成できることがわかった．また，この新しいアルゴリズムの計算量は虚モデルを持つ場合と漸近的に同等であることが証明できた（学会発表①）．一方，このアルゴリズムを実装するにあたって，既存のアルゴリズムで用いられている様々な最適化，例えば終結式の計算や，剰余環を考えることによる多項式因数分解の回避などを適用できるか検討する必要があり，これは今後の課題である．

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計　３件）

① 内田幸寛，超楕円 Jacobi 多様体の Mordell-Weil 群の計算，日本応用数理学会論文誌，査読有，25，(2015)，229-253，DOI:10.11540/jsiamt.25.3_229

② Akihiko Onishi，Yukihiro Uchida，Shigenori Uchiyama，A small secret exponent attack on cryptosystems using Dickson polynomials，JSIAM Letters，査読有，7，(2015)，41-43，DOI: 10.14495/jsiaml.7.41

③ Junichi Yarimizu，Yukihiro Uchida，Shigenori Uchiyama，The elliptic curve Diffie-Hellman problem and an equivalent hard problem for elliptic divisibility sequences，JSIAM Letters，査読有，6，(2014)，5-7，DOI: 10.14495/jsiaml.6.5

〔学会発表〕（計　７件）

① 内田幸寛，種数 2 の超楕円曲線の位数計算と等分多項式，代数幾何学と暗号数理の展開，2017 年 2 月 8 日，九州大学西新プラザ（福岡県福岡市）

② 内田幸寛，ある不定方程式系の解と準エルミート多項式の零点の有理性について，第 12 回代数曲面ワークショップ，2016 年 2 月 6 日，首都大学東京秋葉原サテライトキャンパス（東京都千代田区）

③ 池田崇，内田幸寛，内山成憲，楕円曲線を用いた Multi-Secret Sharing について，日本応用数理学会 2015 年度年会，2015 年 9 月 11 日，金沢大学角間キャンパス（石川県金沢市）

④ 内田幸寛，超楕円 Jacobi 多様体上の標準高さの計算について，Workshop on Computational Number Theory with Implementations 2015，2015 年 2 月 21 日，九州大学伊都キャンパス（福岡県福岡市）

⑤ 内田幸寛，Jacobi 多様体上の標準高さに関するアルゴリズム，数学ソフトウェアとフリードキュメント XIX，2014 年 9 月 24 日，広島大学東広島キャンパス（広島県東広島市）

⑥ 尾西昭彦，内田幸寛，内山成憲，Dickson 多項式を用いた暗号方式に対する秘密鍵が小さい場合の攻撃法，日本応用数理学会 2014 年度年会，2014 年 9 月 4 日，政策研究大学院大学（東京都港区）

⑦ 内田幸寛，代数曲線の数論と暗号への応用，Joint workshop on pure and applied mathematics，2013 年 11 月 1 日，東北大学青葉山キャンパス（宮城県仙台市）

〔その他〕
ホームページ等
http://www.comp.tmu.ac.jp/y-uchida/

６．研究組織
(1)研究代表者
内田　幸寛（UCHIDA, Yukihiro）
首都大学東京・理工学研究科・准教授
研究者番号：90533258