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　３０　年　　６　月　２０　日現在

機関番号：　１２６１１
研究種目：　若手研究(B)
研究期間：　2015～2017
課題番号：　１５Ｋ１６００３

研究課題名（和文）グレブナー基底を用いた楕円曲線上の離散対数問題への解析

研究課題名（英文）Groebner attacks on the discrete logarithm problem over elliptic curves

研究代表者
Ｄａｈａｎ　Ｘａｖｉｅｒ（Dahan, Xavier）

お茶の水女子大学・理学部・学部教育研究協力員

研究者番号：５０５６７５１８

交付決定額（研究期間全体）：（直接経費）　　2,000,000円

研究成果の概要（和文）：幂零元を持つ係数環上のモニックな（一変数）多項式の二つに対して、最大公約数の概念を導入した。これを使って、このような係数環上の多項式を扱う中国剰余定理における「余因子」を計算できた。それで、三角形集合と呼ばれる辞書式順序グレブナー基底の族の一つを計算するときに、生じる係数の増大（ビット長）を見積もった。この中国剰余定理がエルミット補間の一種とみなすことができる。この視点から、より多い利点がある重心型のエルミット補間へ変換する計算を研究し、場合によって成功できた。
上記の新規性をもつ結果は、今まで「根基」の場合に制限されていた結果を一般化し、新しい方向性の研究を開く。

研究成果の概要（英文）：I introduced a new GCD of two monic polynomials defined over rings with nilpotent elements. This was applied to the computation of cofactors (also known as Bezout coefficients) in the Chinese Remainder Theorem for polynomials with coefficients in such rings. Then, this was exploited to estimate the coefficients growth in the computation of a non-radical triangular set (a special lexicographic Groebner basis). This Chinese Remainder Remainder theorem can be seen as a kind of Hermite interpolation. Then we have investigated in some special cases the conversion to the more amenable barycentric form of Hermite interpolation.
This new ability to treat polynomials with coefficients in such rings opens the way to new directions of research, which were limited so far to the "radical" case. Some of these directions are ongoing research.

研究分野：　計算機代数

キーワード：　グレブナー基底　ヘンゼル環　最大公約因数　中国剰余定理

１．　研究開始当初の背景

(1) 2010 年代から、暗号方式、デジタル署名アルゴリズム(DSA)、ペアリング暗号など利用される有限体の拡大体上の楕円曲線に対して、指数計算法という離散対数問題の解読は発展した。特に、二元体の重要なケースが、Petit-Quisquater らによって、「first-fall degree」という仮定として導入された。正しければ初の「準指数時間」のアルゴリズムが対案されたことになる。

２．　研究の目的

(1) それに従って、複数の研究が発表された。そこで、ポイントは連立代数方程式を解くアルゴリズムである。主要なグレブナー基底方法において、その「first fall degree」仮定が正しいかを研究する目的であった。

(2)　私の主な研究分野は、連立代数方程式の計算である。これを活かして、Semaev 多項に対して Weil 降下を行う前に、消去法を行おうとし、幾つかの改善を加えられないかと考えた。

(3) ただ、2015 年に発表された論文
M.-D, Huang, Kosters, Yao “Last fall degree, HFE , and Weil descent attacks on ECDLP” (CRYPTO 2015, pp:581-600)
は、その仮定に対してかなり悲観的な結論を与えた。それ以来、関連の研究は衰退し、この研究課題の重要性も下がっている。

(4) それで、「研究が当初計画どおりに進まない時の対応」で記述したとおり、私はグレブナー基底を中心に研究を続けた。その計画の目的は、（有限体上の）消去法を行うために不可欠な、辞書式順序グレブナー基底に関連するものである。

３．　研究の方法

(1) 一変数の多項式の最大公約因子、中国剰余定理を始め、様々な基礎のアルゴリズムは、多項式の係数は少なくとも、零因子を含まない環とされている。ただ、特別な係数環においては、ある意味では最大公約因子の概念を定義することができる。その特別な環は、零次元の準素イデアルの辞書式順序グレブナー基底 T に対応する剰余環 k[x]/T である。零元でない元は、冪零元あるいは単位元である。ということは、整域でもないが、ある意味では体から離れていない。

(2)そこで、ポイントは上記の剰余環はヘンゼル環であり、モニックな一変数の多項式を互いに素な因数に一意分解できる。従って、精度を下げれば、多項式の二つは共通因数を持つことを証明できる。この精度を定義するために、前述の準素辞書式順序グレブナー基底 T を書き直して、なんとかテーラー展開と類似することを示した、（論文（１））。そこでテーラー展開の階数と同様に、制度の概念を定義した。

４．研究成果

(1) 上記の最大公約因数(英：greatest common divisor=gcd)を理論的に完全に定義した。(雑誌論文(1))。以降の 3.(2)での説明どおりに、準素イデアルの精度が下げるにつれて、最大公約因数の次数は増える。
多項式 a と b の gcd に関しては、イデアル等式<a,b>=<gcd>が求められている一方、精度の依存で、イデアル等式を満たす唯一の gcd がない。従って、精度とそれに対応する gcd をすべて考慮するほかなく、複数 gcd とその精度を出てくるアルゴリズムの概念を提案した。このデータを gcd chain と名付けた。

(2)その gcd を使って、上記の零等元を持つ剰余間の上で、中国剰余定理における「余因子」(英：cofactor) を計算できることを示した(論文(2))。それで中国剰余定理を適用できることになり、互いに素な複数の根基でない特別な辞書式順序グレブナー基底を構成することを、論文(2)も記述した。またさらにこの過程の下で、行われた係数の膨大（ビット長に関する計算量）を見積もった。

(3) また、多項式補間の分野において、定めた点における関数の値からだけでなく、関数の微分における値も扱える Hermite 方式では、重心(英：barycentric)Hermite 方式も知られており、普通の Hermite 補間に比べて利点があるといわれている。例えば前者はより小さな係数がある一方、直接計算するのは難しい。従って、Hermite 方式から重心 Hermite 方式への変換式が求められている。ある意味では、二、三変数多項式補間に対して、雑誌論文(3)はこう変換公式を与えた。

(4) 冪零元を持つ環上の多項式に対して、初めて最大公約因子、中国剰余定理の基礎かつ古典的のアルゴリズムを設計できるようになったことで、さらに複数の方向に向けて研究の可能性が開かれ、新しい結果をもたらすと期待されている。
例えば、中間結果（学会発表(４)、今の時では投稿中）では、ほぼ任意の辞書式順序グレブナー基底を、準素部分から、中国剰余定理に沿って、構成することを示した。

(5) その他、論文（4）では、ポスト量子暗号と呼ばれる次世代公開鍵暗号の候補の一つである「多変数公開鍵暗号」に貢献した。今は NIST(アメリカ国立標準技術研究所)で行われている「ポスト量子暗号の標準化」への公募の背景で、すべての候補を評価するにあたり、提案されるパラメータも見積もる必要がある。提案者にパレメータの選択に関して根拠を与えるために、ストレステストのようなものが望まれる。
そこで多変数公開鍵暗号の安全性を根本となる「連立代数方程式の解求の困難」を明確に見積もる必要がある。どれくらい大きな方程式を解けるかを明らかにするために、我々は MQ-Challenge を設立した。
https://www.mqchallenge.org/
論文(4)と広告のポスタ(9)では、その MQ-Challenge を説明し、世界中の研究者に参加を呼び掛けている。

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 4 件）

(1) DAHAN Xavier、Gcd modulo a primary triangular set in dimension zero. *In Proc. Of ISSAC 2017, Kaiserslautern, Germany.*査読有。*pp:109-116 (2017) ACM press.*

(2) DAHAN Xavier、Bit-size of non-radical triangular sets. In Proc. *MACIS 2017, Vienna, Austria*, 査読有. Lecture Notes in Computer Science, No10693, pp:264-269.

(3) DAHAN Xavier、Bit-size reduction of non-radical triangular set in two and three variables. *In Proc. Of SCSSS 2016, Tokyo, Japan.*査読有 *EPiC Series in Computing, Vol.39 pp:169-182.*

(4) T. Yasuda, X. Dahan, Y.-J. Huang, T. Takagi and K. Sakurai. MQ Challenge: Hardness Evaluation of Solving Multivariate Quadratic Problems, *IACR Cryptology ePrint Archive Report 2015/275.* 査読無。

〔学会発表〕（計 9 件）

(1) X. Dahan. 根基でないイデアルの三角形集合のビット長。RIMS 研究会、2017 年 12 月。京都大学。

(2) X. Dahan. On the bit-size of non-radical triangular sets in dimension zero. MACIS 2017, Teknikum. Vienna, Austria. 2017 年１１月.

(3) X. Dahan. Gcd modulo a primary triangular set of dimension zero. *ISSAC 2017.* (July 25-28, ドイツ)

(4) X. Dahan. Fast construction of a lexicographic Groebner basis of the vanishing ideal of a set of points. *ACA 2017,* (July 18th, High-Performance computing session, エルサレム).

(5) X. Dahan. Cayley graphs based on octonions, and their implementation in Magma. *ACA 2017,* (July 17th, Computer Algebra in Algebraic Graph Theory session, エルサレム).

(6) X. Dahan. On rational solutions of polynomial systems of dimension zero over a finite field. *ACA 2017* (July 21th, Post-Quantum cryptography session. エルサレム).

(7) X. Dahan. 招待チュートリアル Groebner bases: introduction and main algorithms" SCSS'2016 Ochanomizu University, March 28th 2016.

(8) X. Dahan. From lexicographic Groebner bases to triangular sets. *ICIAM 2015, Beijing, China.* (Mini-symposium on Triangular decomposition of polynomial systems: solvers and applications", August 11th 2015.)

(9) X.Dahan. A Multivariate Quadratic challenge toward post-quantum generation cryptography (ポスターを用いて) *ISSAC 2015, Bath, England.*

〔図書〕（計 0 件）

〔産業財産権〕
○出願状況（計 0 件）

名称：
発明者：
権利者：
種類：
番号：
出願年月日：
国内外の別：

○取得状況（計 0 件）

名称：
発明者：

権利者：
種類：
番号：
取得年月日：
国内外の別：

〔その他〕
ホームページ等
https://xdahan.sakura.ne.jp

６．研究組織

(1)研究代表者
ダハングザヴィエ（DAHAN XAVIER）
お茶の水女子大学、理学部　学部教育研究協力員
研究者番号：50567518

(2)研究分担者
（　　）

研究者番号：

(3)連携研究者
（　　）

研究者番号：