立教大学学術推進特別重点資金（立教ＳＦＲ）
大学院学生研究
２０１９年度研究成果報告書

研究科名	立教大学大学院　理学研究科　数学専攻		
研究代表者（2020年3月現在のものを記入）	在籍課程・学年・学生番号 ☐博士前期課程　年 ☑博士後期課程２年 （学生番号：18rc001e　）	氏　名 石原侑樹　印	
指導教員	所属部局・職 理学部　教授	氏　名 横山和弘　印	
自然・人文・社会の別	自然 ・ 人文 ・ 社会	**個人・共同の別**	個人 ・ 共同　名
研究課題	モジュラー技法を用いた計算機代数の新しい理論とアルゴリズムの構築		
研究組織（研究代表者・共同研究者）※2020年3月現在のものを記入	在籍研究科・専攻・課程・学年 理学研究科・数学専攻・博士課程後期課程・２年	氏　名 石原侑樹	
研究期間	２０１９　年度		
研究経費（1円単位）	（支出金額）　146,177円　／（採択金額）　200,000円		

研究の概要（200～300字で記入、図･グラフ等は使用しないこと。）

計算機代数（Computer Algebra）は、計算機科学と数学の境界的領域であり、手計算では難しい様々な数学上の計算を可能にする。数学上の計算の例として、可換環論や代数幾何学においては、標数が0の体を係数とする多項式環における「イデアル操作」などが重要である。例えば、局所化操作や準素イデアル分解は、与えられたイデアルの特徴や代数多様体の構造を考察する上で利用される。それらを実際に計算する上で重要な道具として、グレブナー基底が知られている。本研究では「モジュラー技法」を用いて局所化操作の計算の高速化に向けた新しい理論とアルゴリズムの構築を行なった。特に、標数0の体として有理数体におけるモジュラー計算を考察した。また、他の標数0の体として、p進体係数における効率的なグレブナー基底計算について共同研究を行なった。

キーワード（研究内容をよく表しているものを３項目以内で記入。）

〔 グレブナー基底 〕〔 局所化操作 〕〔 モジュラー技法 〕

研究成果の概要（図･グラフ等は使用しないこと。）

計算機代数は、計算機数学の純粋数学と境界領域であり、手計算では困難な様々な計算を可能にすることを目的としている。その応用範囲は広く、可換環論や代数幾何学、暗号理論、統計学、微分方程式論など、幅広い分野に応用されている。本研究で関連するのは、特に「可換環論」と呼ばれる分野である。可換環論とは、整数の集合や多項式の集合を一般化した「可換環」と呼ばれる数学的対象について研究する分野であり、100 年近くまたはそれ以上の長い歴史がある。可換環論は純粋数学の一分野ではあるが、実用的な面でもその考え方は有用である。例えば、連立方程式を解く際には、対応するイデアルという概念を考えることで、解の情報について分析することができる。

計算機が広く普及されるようになってきてからは、可換環論の計算はコンピュータでも盛んに行われるようになってきた。前述の連立方程式の解の個数や次元もコンピュータを使って計算することができる。可換環論の種々の計算をコンピュータで行う際に重要な役割を果たすものの１つが「グレブナー基底」と呼ばれる概念である。グレブナー基底は簡単にいうと「性質の良い多項式の集合」であり、連立方程式を解きやすい形に変形をしたり次元などの特徴量も計算したりすることができる。例えば、連立方程式 x^2+y^2=1, 2x+3y=2 に対し、イデアル<x^2+y^2-1, 2x+3y-2>の辞書式順序 x>y のグレブナー基底を計算すると、{13y^2-12y, 2x+3y-2}がグレブナー基底の１つとして得られる。ここから、元の連立方程式を変形した連立方程式 13y^2-12y=0, 2x+3y-2=0 が得られる。ここで、13y^2-12y=0 は y だけの方程式であり、因数分解をすると y(13y-12)=0 であるから、y=0, 12/13 が成り立つ。これを 2x+3y-2=0 に代入して x について解けば、x=1, -5/13 となり、元の連立方程式の解、(x, y)=(1, 0), (-5/13, 12/13)を計算することができた。このように、グレブナー基底は性質の良い多項式の集合であるため、連立方程式を解きやすい形に変形することができる。グレブナー基底は、連立方程式の求解の他にもイデアル操作やホモロジー代数の計算などにも用いることができる非常に有用な道具である。

本研究では標数 0 の体上におけるグレブナー基底やイデアル操作の計算の効率的なアルゴリズムについて追究した。標数 0 の体とは、簡単にいうと、1+1=2, 1+1+1=3, 1+1+1+1=4, 1+1+1+1+1=5…というように、1 をどんなに足していっても絶対に 0 にならないような（四則演算ができる）数の体系のことである。私たちが普段慣れ親しんでいる有理数や実数の集合は、標数 0 の体である。それ以外の標数 0 の体としては、p 進体が知られている。有理数から実数を作るためには、絶対値によって完備化をする方法が１つある。完備化とは簡単にいうと、「隙間を埋める」操作である。例えば、有理数には 1 や 1/3 など多くの数があるが、√2 やπなどの無理数はその中には入っていない。しかし、√2 にいくらでも「近い」有理数を取ることができるから、有理数というのにはぎっしり詰まっているように見えて隙間が空いているような数の集合である。そのような隙間を埋めることで実数を構成することができる。ここで、「近さ」というものを考えたが、上で考えているものは絶対値のことである。この「近さ」として別の「近さ」で隙間を埋めれば、有理数を含む別の数の体系を作ることができる。その１つが p 進体である。ここで、p は素数であり、近さとしては、「p の冪をたくさん含むほど小さい」といったような近さを採用している。例えば、p=5 とした時、-5、25 は通常の絶対値では 5 の方が小さいが、p 進絶対値としては 25 の方が小さくなる。言い方を変えると、5, 25, 125, …という 5 冪の数列は p 進絶対値としてはどんどん小さくなるため、p 進距離においては 0 に収束するのである。このように、p 進体というのは、通常とは違う距離が入っていて、その係数を持つグレブナー基底を計算する時も、それを考慮する必要がある。p 進数は一見すると奇妙に見える数かもしれないが、多くの数学者によって研究されている興味深い分野の１つである。

さて、標数 0 の体を係数とする多項式の計算において、一般的に問題の１つとなるのが、「中間係数膨張」である。中間係数膨張は、入力と出力に出てくる多項式の係数が小さいのにも関わらず、入力から出力を計算する過程で係数が膨張してしまう現象である。係数が膨張すると計算に多くの時間がかかったり、コンピュータのメモリが足りなくなったりする問題が生じる。例えば、イデアル <8x^2y^2+5xy^3+3x^3z+x^2yz, x^5+2y^3z^2+13y^2z^3+5yz^4, 8x^3+12y^3+xz^2+3, 7x^2y^4+18xy^3z^2+y^3z^3> の次数付逆辞書式順序による簡約グレブナー基底は、<x, y^3+1/4, z^2>であるが、それをブッフベルガーアルゴリズムなどで計算すると、計算途中で約 8 万桁の係数が登場してしまうことが知られている。これは、入力と出力の係数の大きさに比べると明らかに中間の係数が膨張していることが分かる。この問題を解決する手法の１つとして、「モジュラー技法(Modular Techniques)」がある。これは有理数体上の計算を、有限体上で代わりに行うことで係数の膨張を回避する手法である。有限体とは、数が有限個しかない数の体系であり、例えば、F2={0, 1}は最も位数が小さい有限体である。F2 においては、0+0=0, 1+0, 1*1=1, 1+1=0 などの関係が成り立っており、有理数や実数と同じように四則演算ができる。ただ、有理数などと異なる点は、標数が 0 ではないというところだ。ここで標数が p であるとは、p 個の 1 の和が 0 になることを意味している（厳密には p-1 個以下の 1 の和が 0 にならないことも仮定)。F2 は 1+1=0 なので標数が 2 の有限体である。素数 p に対し、標数 p の有限体が存在することが知られており、すなわち、有限体は無限に存在する。有限体は数が有限個しかないため中間係数膨張は起きない（正確には、上限があるため有理数の場合に比べ膨大な係数になることはない)。

研究成果の概要　つづき

研究代表者はこのモジュラー技法の局所化操作の効率的な計算への応用を行った。局所化操作とは、イデアル商や飽和イデアルなど、簡単にいうとイデアルから特定の情報を取り出すような操作である。例えば、(x-y)(y-(x+1)^3)(y^2-x)(x^2-y^2-1)=0 で定義される曲線を考える。この曲線はそれより細かい複数の曲線 x-y=0, y-(x+1)^3=0, y^2-x=0, x^2-y^2-1=0 からできている。この中から原点を通るものだけを取り出したい場合、幾何的には原点の周りで局所化をすれば良い。すると、(x-y)(y^2-x)=0 という式が取り出せ、特定の情報だけを抽出することができる。実際、I=<(x-y)(y-(x+1)^3)(y^2-x)(x^2-y^2-1)>として、極大イデアル m=<x,y>により、二重の飽和イデアル(I:(I:m^∞)^∞))を計算すれば、(I:(I:m^∞)^∞))=<(x-y)(y^2-x)>が得られる。研究代表者は特に二重イデアル商についてモジュラー技法が適用できないか考察した。二重イデアル商は、イデアル商(I:J)が二重になったイデアル(I:(I:J))で、素因子の判定や equidimensional hull の計算に用いることができる。さらに、その変種は準素成分の判定や孤立準素成分の生成に用いることができる。準素イデアル分解は簡単にいうと因数分解を一般化したものであり、可換環論や代数幾何学の基本的な道具の１つとなっている。このように、二重イデアル商とその変種は局所化操作の計算に利用することができるが、その効率的な計算が問題になっている。そこでモジュラー技法を適用して高速化を図ろうといたった次第である。

モジュラー技法について詳細を述べる。まず有理数体上で行いたい計算を複数の有限体上で並列に計算し(Step.1)、次にそれらを中国人剰余定理 (CRT) や rational reconstruction などで有理数体上に構成する(Step.2)。最後に、その構成した結果が本当に正しいかどうかを判定法により確かめる(Step.3)。有限体においては中間係数膨張が起きないため、Step.1 の計算は有理数計算に比べ高速に行えることが期待できる。Step.2 については、あくまで計算できるのは答えの「候補」であることに注意が必要である。有理数と有限体の計算は必ずしもうまく対応がついているわけではなく、lucky な素数と lucky でない素数が存在する。Lucky でない素数は有限個しかないことが知られているが、これはアプリオリ（事前）に知ることはできない。そこで、Step.3 で答えの候補が本当に正しいかどうかを判定することが重要となってくる。Step.1,Step2 は、他のモジュラー技法の応用とほとんど似たようなものになるので、Step.3 が特に局所化操作への適用に向けて改良をするべき点となってくる。

研究代表者は、(二重) イデアル商と飽和イデアルに対して、先行文献を参考にモジュラー技法の Step.3 の新しい判定法を考案し、数式処理ソフト Singular での実装を行った。イデアル商や飽和イデアルについては、先行文献では(I:f)、(I:f^∞)と割る側が多項式であったものを、(I:J)、(I:J^∞)のようにイデアルに一般化を行った。加えて二重イデアル商(I:(I:J))に対しても判定法や CRT を一部除去できる素因子の判定法を発見した。詳細については、プレプリントとして、https://arxiv.org/abs/2003.00496 で公開もされている。また、数式処理ソフト Singular において、モジュラー技法を用いた局所化操作のアルゴリズムを実装した。Singular は世界的な数式処理ソフトであり、多くの研究者が利用している。私が実装したアルゴリズムは Singular の github のリポジトリ https://github.com/Singular/Sources/blob/spielwiese/Singular/LIB/moddiq.lib でも公開されている。また、計算機実験を行ったところ、実際にモジュラー技法が効果的に働いている例がいくつか発見されている。この研究成果については、九州大学で行われた「Software in Mathematics Demonstration Track in Hakata Workshop 2020」でポスター発表を行った。色々な参加者の方と意見交流を行い、自分の研究にも非常に有益な情報を得ることができた。

最後に、有理数以外の標数 0 の体として、p 進体係数のグレブナー基底の計算について共同研究を行った。共同研究は、Limoges 大学の Tristan Vaccon 講師と立教大学の横山和弘教授との３人で行った。9 月から 10 月にかけて、合計約３週間フランスの Limoges 大学に研究出張を行った。フランスに共同研究で少し長い出張を行ったのは研究代表者にとって初めての経験であった。先方の大学の研究者とも色々と交流ができ、とても貴重な経験であった。さて、グレブナー基底の計算アルゴリズムの１つとしては、FGLM アルゴリズムと呼ばれるものが広く知られている。今回、共同研究ではこれを p 進体などの付値を含む係数においての一般化を考察した。付値を考慮すると係数によって先頭項が変わってしまうので、アルゴリズムを考える際にとても複雑になる。共同研究の成果は論文として投稿済みで現在査読中である。研究代表者はこの p 進体においてもモジュラー技法を適用しようと考えていたが、今回の研究ではそこまで至らなかった。これは今度の課題にしたいと思っている。

以上のように、モジュラー技法を用いた局所化操作の新しい判定法とそのアルゴリズムの実装を行うことができた。計算機実験ではいくつかの例で効果的に機能していて、また誰もが利用できるように実装を公開しているため、世界中の研究者の研究に貢献できれば幸いである。また、p 進体についてはモジュラー技法を適用するまでにはいたらなかったが、グレブナー基底のアルゴリズムについては共同研究で共著論文として投稿することができた。

※この（様式２）に記入の成果の公表を見合わせる必要がある場合は、その理由及び差し控え期間等を記入した調書（Ａ４縦型横書き１枚・自由様式）を添付すること。

研究発表（研究によって得られた研究成果を発表した①～④について、該当するものを記入してください。該当するものが多い場合は主要なものを抜粋してください。なお、成果発表を確認できる資料を合わせて提出してください。）

①雑誌論文（著者名、論文標題、雑誌名、巻号、発行年、ページ）
②図書（著者名、出版社、書名、発行年、総ページ数）
③シンポジウム・公開講演会等の開催（会名、開催日、開催場所）
④その他（学会発表、研究報告書の印刷等）

① 該当なし
② 該当なし
③ 該当なし
④ Software in Mathematics Demonstration Track in Hakata Workshop 2020、2020年2月21日、石原侑樹「Modular Techniquesを用いた効率的な局所化操作の計算」、九州大学伊都キャンパス