公開

研 究 終 了 報 告 書

「Kudla 予想の解決及び志村多様体の研究と暗号への応用」

研究期間： 2020 年 11 月～2023 年 3 月
研 究 者： 前田 洋太

1． 研究のねらい

本研究提案では志村多様体に関する予想である Kudla 予想と、それらの性質の解明及び耐量子計算機暗号への応用をねらいとしている。Kudla 予想は Kudla-Millson により定式化された予想で、コンパクト志村多様体上の部分志村多様体の交点数を並べた関数が保型形式になるということを主張している (IHES. Publ. Np.71 (1990))。しかしこの論文で扱われている志村多様体は限定的であり、数論的応用を考える上でいくつかの問題点が存在した。特にノンコンパクト志村多様体についての Kudla 予想は研究が困難で Bruinier-Zemel (arXiv:1912.1185, 2019)以外には研究が進んでいない。加えてこの論文では特殊な志村多様体に関して、その上余次元 1 の部分多様体についてしか考察されていない。この結果では数論的応用、特に L 関数との関わりを調べる上で不十分であり、より一般的に予想を解決する必要がある。提案者は自身がコンパクトな場合に解決したような一般的な志村多様体についてこの問題を考察し、より高い余次元をもつ部分志村多様体について予想を定式化、解決することを一つの目標としている。また、志村多様体自身の幾何学的性質を調べることは代数幾何学において重要な問題であり、提案者は保型形式等の数論的手法を用いてこの問題に取り組み、最終的に志村多様体の分類理論に一つの区切りをつけることをねらいとしている。

さらに、志村多様体を耐量子計算機暗号の研究に応用することもねらいの一つである。具体的には志村多様体を用いた暗号方式提案を行う。秋山-後藤(IEICE Tech. 104,421(2004))は代数曲面の求切断問題の困難性を用いた代数曲面暗号を構成した。この暗号には簡約やトレース写像による攻撃法が存在しており(岩見,内山-徳永,Voloch)、変数を増やすことで改良した代数曲面暗号が考案された(Lecture Notes in Comput. Sci., 5442(2009))。この代数曲面暗号を元に非線形方程式の最小解を用いた暗号、非線形不定方程式暗号が考案された(Lecture Notes in Comput. Sci., 10719(2018))。この暗号は IE-LWE 仮定の下で IND-CPA 安全な準同型暗号であり、耐量子暗号の候補である。さらに格子暗号と比較して鍵長が短くてすむという利点がある。ここで代数曲面暗号の説明をする。これは曲線 C の上に曲面（曲線の族）S が乗っている状態(S¥rightarrowC)を考え、その切断を求めることが曲線の有理点を求めることと同程度に困難であるという事実に安全性の根拠を置いている暗号であり、楕円曲線暗号や RSA 暗号とは本質的に異なる。本研究で考察する志村多様体をこの暗号に応用する。具体的にはモジュライ空間をなすノンコンパクト志村多様体 X に対してその上に普遍的な幾何学的対象の族 U が乗っているという、上記と同じ構図 U¥rightarrowX を用いる。例えば U として Abel 多様体や K3 曲面の族を取ることができ、既存の代数曲面暗号の高次元化を考察できる。これを志村多様体暗号と呼び、さらに提案者はこの暗号を発展させた非線形不定方程式暗号を開発する。この暗号は既存のものよりも変数が増えるので攻撃に対する耐性が強いと考えられる。また代数曲面暗号は電子署名に応用される(SCIS 2010)ので、上記の暗号のゼロ知識証明、電子署名への応用を考察する。

2. 研究成果

（1）概要

Kudla 予想に関してはノンコンパクト志村多様体に関する考察は成果として発表できなかったものの、その過程でコンパクトなユニタリ型志村多様体に関する研究を進めることができ、結果として査読付き論文を一件発表した。これは既に証明された場合の Kudla 予想に対する別証明を与え、さらには既存の枠組みを一般化する形でより広いクラスのユニタリ型志村多様体に対して予想を解決した。本研究を元に、今後既存の数論的手法の幾何学化が研究されていくと考えられる。

志村多様体の性質に関しては、査読付き論文二件とプレプリント二件を発表した。それらの概略を順に概説すると、まずはボール商の上の不正則カスプに関する研究である。不正則カスプはモジュラー曲線において盛んに研究されている対象であり、その高次元化の定式化及びその系としてボール商の小平次元への影響を考察した。また、不正則カスプの分類及び直交型モジュラー多様体上のカスプとの関係も明らかにした。次に尾高悠志氏との共同研究において志村多様体の双有理幾何学的性質を鏡映的保型形式の観点から明らかにした。鏡映的保型形式は代数幾何学、整数論、表現論において異なる角度から研究され続けてきた。本論文ではより強い概念である特殊鏡映的保型形式を定義し、その存在が志村多様体の Satake–Baily–Borel コンパクト化の双有理的性質に与える現象について考察した。特に、その応用として（ログ）エンリケス曲面のモジュライ空間が Fano 多様体になることを示した。プレプリントに関しては、一方はボール商の上の分岐因子から生じる障害を考察したものである。ボール商の次元が大きいとき、それが一般型になるという定理を示すことを考えると、特異点から生じる障害、分岐因子から生じる障害、及び尖点形式の存在から生じる障害が挙げられる。このうち特異点から生じる障害は Behrens 氏によって解決されている。本研究ではボール商の次元が十分大きいとき、分岐因子から生じる障害の影響が十分小さいことを示した。最後に、Klaus Hulek 氏と共同で、P^1 上の 8 点のモジュライ空間のコンパクト化の分類を行った。

暗号研究に関しては、志村多様体暗号の考察及び SIDH の高次元化と高速化に関する研究を行った。論文発表という形では成果は出なかったが、研究集会で講演を行い、今後も研究を続けていく予定である。

（2）詳細

Kudla 予想に関して：

ユニタリ型志村多様体の Kudla 予想は Liu、Kudla–Millson らによって研究されてきた。本研究提案では Bruinier の手法を用いることで Liu の証明に別証明を与え、さらに自身が直交型志村多様体の研究を行う際に用いた手法を援用することで彼らの結果を一般化する結果を得た。

志村多様体の幾何学的性質に関して:
主要な研究をピックアップすると、ボール商の上の不正則カスプの定式化を行ったことで、ユニタリ型志村多様体の小平次元の計算を行うための low slope cusp form trick と呼ばれる判定法を証明することができた。これは直交型志村多様体上について証明されていた判定法の類似であり、今後有用になってくると考えられる。また、ユニタリ型志村多様体の分岐に関する障害の研究は、分類理論を推し進める上で必要な研究であり、本研究提案の目標としていた研究の一つである。手法について詳しく述べると、性質の良い保型形式(reflective modular forms, quasi-pullback of Borcherds form)を用いて Gritsenko-Hulek-Sankaran 氏による判定法をユニタリの場合に用い、Hirzebruch-Mumford volume を Prasad の公式により計算した。これは直交型志村多様体に関する先行研究では Gritsenko-Hulek-Sankaran 氏により Hirzebruch-Mumford volume の計算及び保型形式の空間の次元の計算を通して小平次元の計算がなされており、馬氏により一般化されている。
暗号への応用研究に関して:
SIDH、及び CSIDH に関しては三菱電機の相川勇輔氏と、非可換群暗号に関しては先述の相川氏及び愛媛大学の加藤元子氏と勉強会、共同研究を行った。

3. 今後の展開

5 年程度のスパンで論文化及び社会実装に取り組んでいきたい。

4. 自己評価

独創的及び挑戦的なアイデアによって問題解決に取り組むことができた。その過程で、分野を超えた様々な研究者との交流を通し研究者ネットワークを構築することができた。一方で、元々掲げていた暗号研究に関しては目標達成において不十分な箇所があると考えられるので、本事業後の研究において達成していきたい。

5. 主な研究成果リスト

(1)代表的な論文(原著論文)発表

研究期間累積件数:3件

1. Yota Maeda, *Modularity of special cycles on unitary Shimura varieties over CM-fields,* Acta Arith. 204(2022), no. 1, 1-18.

本研究課題では志村多様体に関する Kudla 予想の解決を一つの目標としていた。本論文ではユニタリ型志村多様体に対する Kudla 予想を考察し、今まで知られていた場合の別証明を与え、さらには既存の枠組みを一般化する形でより広いクラスのユニタリ型志村多様体に対して予想を解決した。本研究を元に、今後既存の数論的手法の幾何学化が研究されていくと考えられる。

2. Yota Maeda, *Irregular cusps of ball quotients,* Math. Nachr (2022, in press).
モジュラー曲線上の不正則カスプは、その幾何学及びモジュラー形式の次元公式への寄与の観点から数論において重要な対象であった。本論文ではその高次元化に当たるボール商において同様の現象が起きうることを示し、その系として小平次元への影響を考察した。また、不正則カスプの分類及び直交型モジュラー多様体上のカスプとの関係も明らかにした。
3. Yota Maeda, Yuji Odaka, *Fano Shimura varieties with mostly branched cusps,* Springer Proceedings in Mathematics & Statistics (PROMS, volume 409) (2022, in press).
鏡映的保型形式は代数幾何学、整数論、表現論において異なる角度から研究され続けてきた。本論文ではより強い概念である特殊鏡映的保型形式を定義し、その存在が志村多様体の Satake-Baily-Borel コンパクト化の双有理的性質に与える現象について考察した。特に、その応用として(ログ)エンリケス曲面のモジュライ空間が Fano 多様体になることを示した。

(2)特許出願

無し。

(3)その他の成果(主要な学会発表、受賞、著作物、プレスリリース等)

1. Klaus Hulek, Yota Maeda, *Revisiting the moduli space of 8 points on P^1*, preprint.
2. Yota Maeda, Reflective obstructions of unitary modular varieties, preprint.