数理・情報のフロンティア
2020 年度採択研究代表者

2020 年度
年次報告書

前田 洋太

京都大学 大学院理学研究科
大学院生(修士課程)

Kudla 予想の解決及び志村多様体の研究と暗号への応用

§1. 研究成果の概要

研究計画に記載した内容のうち、志村多様体の不変量の計算とそれに伴う分類理論の開拓及び耐量子計算機暗号の研究を行った。

志村多様体の不変量、特に小平次元の計算については志村多様体が一般型になるというタイプの研究から単繊織になるというタイプまで幅広く扱った。それに関して論文発表、学会発表を行い最終的に修士論文に内容をまとめた。今後の展望として小平次元より深い分類に関する手がかりを得た。その点に関しては次年度に論文としてまとめる予定である。

耐量子計算機暗号に関しては、特に SIDH の高速化と新たな hash 関数の構成に取り組んだ。SIDH の高速化についてはねじれ点を高速に求めるアルゴリズムを 1 次元志村多様体であるモジュラー曲線の観点から考察した。また、代数幾何を用いて既存の hash 関数の機能性向上に努めた。

【代表的な原著論文情報】

- Yota Maeda. Modularity of special cycles on unitary Shimura varieties over CM-fields. arXiv:2101.09232 (preprint). January 2021.