研（様式１６－２号）

2012　年度　中央大学特定課題研究費　－研究報告書－

所属	理工学部	身分	教授
氏名	諏訪　紀幸		
NAME	SUWA Noriyuki		

１．研究課題

（和文）代数学、特に整数論におけるアルゴリズム

（英文）Algebra, and Algorithms in Number Theory

２．研究期間

２年間

３．研究の概要（背景・目的・研究計画・内容および成果　和文 600 字程度、英文 50words 程度）

（和文）本研究では、(1) 整数論に現れるアルゴリズムの収集と精査、その実装、(2) 有限体に関するアルゴリズムの収集と精査、その実装、(3) アルゴリズムの実行とデータの蓄積、(4) 理論的な考察、を課題とした。

一昨年度は５人の修士論文作成を指導したが、その中の３人がアルゴリズムの理解とプログラミング作成に取り組んだ。「有限体において平方根を求める Tsz-Wo Sze のアルゴリズ」「有限体の上に定義された楕円曲線さらに超楕円曲線に関わるアルゴリズム「擬似乱数生成アルゴリズム Mersenne Twister」に関する総合報告であったが、いずれも修士論文作成にあたって参考にした論文に展開されている議論を数学として裏付け、そこで提唱されているアルゴリズムを実際に実装した。学会発表までは持って行けなかったが、アルゴリズムを受け売るだけではなく実際にプログラムを組むに当たっては数々の困難を克服しなければならなかった。

昨年度は整数論や有限体の上の代数曲線に関連するアルゴリズムの取材に努めた。特に、２０１４年１月に鹿児島で開催された情報セキュリティと暗号に関する総合研究集会 SCIS2014 では多くの知見を得た。

（英文）The main subjects of the research are as follows: (1) to study and analyze algorithms in the number theory, including implementations; (2) to study and analyze algorithms concerning finite fields, including implementations; (3) to accumulate data with the aids of implemented algorithms; (4) to advance theoretical considerations.

４．おもな発表論文等（予定を含む）

【学術論文】（著者名、論文題目、誌名、査読の有無、巻号、頁、発行年月）

[1] N. Suwa, Artin-Schreier-Witt extensions and normal bases. Hiroshima Math. J.,査読有, 44 巻, 325354 (2012)

【学会発表】（発表者名、発表題目、学会名、開催地、開催年月）

[1] 諏訪紀幸, Kummer theory for algebraic tori and normal basis problem. 早稲田大学整数論研究集会, 早稲田大学, '13.3.16

[2] Kummer theory for algebraic tori and normal basis problem: some examples. 福岡数論研究集会, 九州大学, '13.8.10

【図　　書】（著者名、出版社名、書名、刊行年）

[1] 木田正雅, 諏訪紀幸, 小林真一 (共編), 京都大学数理解析研究所, Algebraic Number Theory and Related Topics 2010. RIMS Kokyuroku Bessatsu B32 (2012)

[2] 諏訪紀幸, 志甫淳, 佐藤周友 (共編), 京都大学数理解析研究所, Algebraic Number Theory and Related Topics 2011. RIMS Kokyuroku Bessatsu B44 (2013)

【その他】（指導修士論文）

[1] 阿部隼大, 有限体における平方根の計算法について

[2] 山口将史, 超楕円曲線の Ate ペアリングについて

[3] 山田雅哉, 擬似乱数生成器 Mersenne Twister について