

機関番号：12601

研究種目：基盤研究（A）

研究期間：2007～2010

課題番号：19204002

研究課題名（和文）数論・幾何の新展開：数論的トポロジー、圏論的数論幾何、アルゴリズム

研究課題名（英文）New developments in number theory and geometry: arithmetic topology, categorical arithmetic geometry, algorithm

研究代表者

松本 眞 (Matsumoto Makoto)

東京大学・大学院数理科学研究科・教授

研究者番号：70231602

研究成果の概要（和文）：

(1)幾何的トポロジーの手法を数論幾何で展開することにより、トポロジーの知見（写像類群のコホモロジーなど）を数論幾何（外ガロア作用など）の研究に応用した。(2)数論幾何の対象を、組み合わせ群論および圏論的に再構築する理論を展開した。(3)代数的・幾何的アルゴリズムを開発し、擬似乱数評価法などの実用数学に応用した。

研究成果の概要（英文）：

By using methods of geometric topology in arithmetic geometry, knowledges on topology (such as the cohomology of the mapping class groups) are utilized in researches on arithmetic geometry (such as outer Galois representations). (2) We developed a frame work to detect objects in arithmetic geometry by means of its combinatorial and categorical data. (3) We developed algebraic and geometric algorithm for applications such as evaluation of pseudorandom number generators.

交付決定額

（金額単位：円）

	直接経費	間接経費	合計
2007年度	7,500,000	2,250,000	9,750,000
2008年度	6,200,000	1,860,000	8,060,000
2009年度	6,300,000	1,890,000	8,190,000
2010年度	6,300,000	1,890,000	8,190,000
年度			
総計	26,300,000	7,890,000	34,190,000

研究分野：数物系科学

科研費の分科・細目：数学・代数学

キーワード：数論幾何学

## 1. 研究開始当初の背景

数論と幾何学は、古代より絡みあいつつ発展してきた。19世紀にはミンコフスキーの「数の幾何」に見られるように、「実数の離散部分集合としての整数」に対して、実幾何学的手法による研究が発達した。一方、1960年代にグロタンディークにより導入されたスキーム理論は、実数のトポロジーから全く離れ、整数や有限体など離散的な環に対しても良いトポロジーを導入してコホモロジー理論を展開するものであり、80年代から

90年代に急速に発展しヴェイユ予想やフェルマー予想の解決という非常に大きな成果をあげた。この流れは、スズリン・ヴォイヴォツキーらによるスキームのホモトピー理論へと受け継がれた。ヴォイヴォツキーは90年代後半に、代数多様体の普遍的なコホモロジー理論である「モチーフの圏」を構成し、ミルナー予想の重要な部分を解決しフィールズ賞を受賞した。この理論は高階ホモトピー理論のモデル圏により定式化され、最先端の研究者が集まる数論幾何の主流の一つで

あった。一方、もともとのトポロジーにおいては、低次元多様体のモジュライや基本群など、幾何的トポロジーが急速な展開を見せた。

## 2. 研究の目的

本研究の目的は、数論における幾何学的手法に、新展開をもたらすことであつた。具体的には、(1) 幾何的トポロジーの手法：基本群やモジュライ空間の幾何を利用した数論幾何・モチーフ理論の展開、(2) 圏論に基づく数論幾何：幾何的対象やその性質を圏論的データから再構成することにより、スキーム論より大きな数論幾何研究の枠組みを構築、(3) 数論・代数学における、幾何的アルゴリズムの開発と応用：冪級数体のノルムに関するレンストラのアルゴリズムや既約性判定アルゴリズム、の3つの連関分野を中心に研究を展開させる。

これらを通じて、モジュライ空間など多様体の数論的基本群におけるガロア表現・ホッジ理論・モチーフ理論の研究、ABC予想へのアプローチ、アルゴリズムを用いた純粋数学研究ならびに幾何的アルゴリズムの工学的応用の研究を行うことであつた。

## 3. 研究の方法

上記(1)については曲線のモジュライ空間の数論的基本群である、数論的写像類群の構造の研究を米国・デューク大学リチャード・ヘイン教授と松本が共同研究を展開した。(2)については望月がABC予想解決への圏論的数論幾何によるアプローチ(フロベニウス作用とガロア圏を融合させた概念であるフロベニオイドを用いてテータ関数を圏論的に再構成することにより、ガウス極を評価する)を進めた。(3)については米国 Art Owen 教授らと松本、西村が共同研究を進めた。海外招聘、国際・国内研究集会を開催するなどの人的交流に加え、アルゴリズム開発に必要なハードウェア・ソフトウェア・人材の確保を行った。

## 4. 研究成果

研究計画の概要でのべた(1)に関して、Hain-松本は曲線のモジュライ空間の幾何的基本群の相対  $\text{pro-1}$  完備化への、トレリ群からの自然な写像が  $\text{pro-1}$  完備化後は単射にならないことを示し、また、ガロア作用が1の外で不分岐であることを示した。(次項論文③) また、松本は Hain-Reed、森田茂之のトポロジー的結果を用いて、曲線上で基本群へのガロア外作用とガロア作用に差がある点が稠密である例を構成した(論文①)。松本は、曲線の基本群に付随するガロア表現について、自己同型群でのガロア群の像と、外部自己同型でのそれがほとんどの点で一致しないことを示した。成果はアメリカ数学会紙 Proceedings of AMS に掲載された。また、Hain 氏との共同研究で、楕円曲線の普遍族の基本群に付随するガロア表現に Eisenstein 保型

形式が現れることを示し、2010年10月に開かれた数理解析研究所国際研究集会にて発表した。玉川は Saidi との共同研究により、正標数での Grothendieck 予想の Hom 版の成立する場合について研究し、成果は Algebra and Number Theory に掲載予定となった。斎藤秀司は  $p$  進体上での零サイクルの有限性を佐藤周友と示し、成果は Annals of Mathematics に掲載された。また、斎藤秀司はコホモロジー論的 Hasse 原理について、ICM にて招待講演を行った。木村は Chow 群論的ゼータ関数が  $A^1$  ホモトピーで有理的になる例を構成し、フランスポワンカレ研究所にて口頭発表を行った。島田、高橋宣能は射影平面の巡回分岐被覆となるある代数曲面上の分岐 divisor が生成する部分格子の原始性を多くの場合に示した。成果は Comment. Math. Univ. St. Pauli に掲載された。(2)について(1)とも関連して、望月は semi graph of anabelioid という profinite 群論とグラフ理論を融合した対象を考え、数論的代数曲線の情報を組み合わせ論的・圏論的に再構築する理論を構築しつつある。その一つの結果として、コンパクト代数曲線の基本群へのガロア作用の忠実性という長年の予想が肯定的に解決された(星裕一郎氏との共同研究、受理済み。)(3)について、原瀬一松本一斎藤睦夫は、疑似乱数評価のためのラティスリダクションアルゴリズムを改善し、10倍以上の高速化に成功した(論文②)。この成果を利用して、松本は斎藤睦夫とグラフィックプロセッサ向き並列乱数発生アルゴリズムを開発し、8月ワルシャワでの国際研究集会にて発表した。論文は投稿中である。

これらの成果は、ICM2010、ケンブリッジ大学・ボルドー大学・東京大学・韓国 KIAS などにおいて開かれた国際研究集会における招待講演として発表されるなど、国際的にインパクトの強い研究となっている。

今後の展望として、(1)については基本群から得られるモチーフへの展開、(2)については数論幾何における未解決予想へのアプローチ、(3)については超一様分布点列の設計への応用、が考えられる。

## 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34件)

① Makoto Matsumoto, "Difference between Galois representations in automorphism and outer-automorphism groups of a fundamental group" Proceedings of the AMS, accepted. 139 (2011), 1215-1220 査読あり。

② Shin Harase, Makoto Matsumoto, Mutsuo Saito, Fast lattice reduction for  $F_2$ -linear pseudorandom number

generators, Mathematics of Computation 80 (2011), 395-407. 査読有

③ Richard Hain, Makoto Matsumoto. 査読有 "Relative Pro- $l$  Completions of Mapping Class Groups," Journal of Algebra, vol. 321 (2009), pp. 3335-3374.

④. Hiroshi Haramoto, Makoto Matsumoto. 査読有 "A  $p$ -adic algorithm for computing the inverse of integer matrices," Journal of Computational and Applied Mathematics 225 (2009), pp. 320-322.

⑤7. Mutsuo Saito, Makoto Matsumoto. "A PRNG specialized in double precision floating point numbers using an affine transition," in: Monte Carlo and Quasi-monte Carlo Methods 2008, 査読有 P. L'Ecuyer and A. Owen (Ed.), Springer-Verlag 2009. pp.589--602.

⑥ Cadoret, Anna; Tamagawa, Akio Stratification of Hurwitz spaces by closed modular subvarieties. Pure Appl. Math. Q. 5 (2009), no.1, 227-253 査読有

⑦ Mochizuki, Shinichi The étale theta function and its Frobenioid-theoretic manifestations. Publ. Res. Inst. Math. Sci. 45 (2009), no. 1, 227-349 査読有

⑧ Elizondo, E. Javier; Kimura, Shun-Ichi Irrationality of Motivic series of Chow varieties. Math. Z. 263 (2009), no. 1, 27-32. (査読有り)

⑨ Chiarellotto, Bruno; Tsuzuki, Nobuo Logarithmic growth and Frobenius filtrations for solutions of  $p$ -adic differential equations. J. Inst. Math. Jussieu 8 (2009), no. 3, 465--505. (査読有り)

⑩ Haramoto, H., Nishimura, T., Matsumoto, M., Panneton, F, L'Ecuyer, P. "Efficient Jump Ahead for  $F_2$ -linear Random Number Generators" INFORMS Journal of Computing, 20 (3), pp.385-390 (2008).

[学会発表] (計40件)

① 松本 眞 "Universal mixed elliptic motive and derivation algebra of the fundamental group of one-punctured elliptic curve" The 3rd MSJ-SI: Development of Galois-Teichmüller Theory and Anabelian Geometry, RIMS Kyoto University. (with Richard Hain) 2010年10月29日

② 松本 眞 学会名

Torsion of abelian schemes and rational points on moduli spaces

タイトル

Differences between Galois representations in outer-automorphisms

of  $\pi_1$  and those in automorphisms, implied by topology of moduli spaces

フランス・ボルドー第一大学

2010年1月28日

③ 松本 眞

学会名 Geometry and Analysis of Automorphic Forms of Several Variables

タイトル

Study of Galois representations via

Teichmüller modular groups.

場所・東京大学数理科学研究科

2009年9月16日

④ 松本 眞

学会名 Anabelian Geometry

タイトル

Differences between Galois representations in automorphism and outer-automorphism groups of the

fundamental group of curves

場所イギリス・ケンブリッジ大

2009年8月28日

⑤ 玉川安騎男

学会名 Anabelian Geometry

タイトル

Torsion of abelian schemes and rational points on moduli spaces

場所イギリス・ケンブリッジ大

2009年8月27日

⑥ 松本 眞

学会名 Asian Conference on Arithmetic Geometry 2007,

タイトル

Relative pro- $l$  completion of fundamental groups'

場所韓国 Korea Institute of Advanced Study.

2007年9月15日

## 6. 研究組織

### (1) 研究代表者

松本 眞 (MATSUMOTO MAKOTO)

東京大学・大学院数理科学研究科・教授

研究者番号：70231602

### (2) 研究分担者

玉川 安騎男 (TAMAGAWA AKIO)

京都大学・数理解析研究所・教授

研究者番号：00243105

(H19→H20: 連携研究者)

望月 新一 (MOCHIZUKI SHINICHI)

京都大学・数理解析研究所・教授

研究者番号：10243106

(H19→H20: 連携研究者)

都築 暢夫 (TSUZUKI NOBUO)

東北大学・大学院理学研究科・教授

研究者番号：10253048

(H19→H20:連携研究者)  
木村 俊一 (KIMURA SHUNICHI)  
広島大学・大学院理学研究科・教授  
研究者番号: 1 0 2 8 4 1 5 0  
(H21→H22:連携研究者)  
寺杣 友秀 (TERASOMA TOMOHIDE)  
東京大学・大学院数理科学研究科・教授  
研究者番号: 5 0 1 9 2 6 5 4  
(H19→H20:連携研究者)  
森田 茂之 (MORITA SHIGEYUKI)  
東京大学・大学院数理科学研究科・名誉教授  
研究者番号: 7 0 0 1 1 6 7 4  
(H19→H20:連携研究者)  
広瀬 進 (HIROSE SUSUMU)  
佐賀大学・理工学部・准教授  
研究者番号: 1 0 2 6 4 1 4 4  
(H19→H20:連携研究者)  
盛田 健彦 (MORITA TAKEHIKO)  
大阪大学・大学院理学研究科・教授  
研究者番号: 0 0 1 9 2 7 8 2  
(H20→H21:連携研究者)  
吉野 正史 (YOSHINO MASAFUMI)  
広島大学・大学院理学研究科・教授  
研究者番号: 0 0 1 4 5 6 5 8  
(H21→H22:連携研究者)  
永井 敏隆 (NAGAI YOSHITAKA)  
広島大学・大学院理学研究科・教授  
研究者番号: 4 0 1 1 2 1 7 2  
(H21→H22:連携研究者)  
須川 俊幸 (SUGAWA TOSHIYUKI)  
東北大学・大学院情報科学研究科・教授  
研究者番号: 3 0 2 3 5 8 5 8  
(H19→H20:連携研究者)  
高橋 宣能 (TAKAHASHI NOBUYOSHI)  
広島大学・大学院理学研究科・助教  
研究者番号: 6 0 3 0 1 2 9 8  
(H21→H22:連携研究者)  
金子 昌信 (KANEKO MASANOBU)  
九州大学・大学院数理学研究院・教授  
研究者番号: 7 0 2 0 2 0 1 7  
(H19→H20:連携研究者)  
田口 雄一郎 (TAGUCHI YUICHIROU)  
九州大学・大学院数理学研究院・准教授  
研究者番号: 9 0 2 3 1 3 9 9  
(H19→H20:連携研究者)  
伊藤 浩行 (ITO HIROYUKI)  
広島大学・大学院工学研究科・准教授  
研究者番号: 6 0 2 3 2 4 6 9  
(H21→H22:連携研究者)  
西村 拓士 (NISHIMURA TAKUJI)  
山形大学・理学部・准教授  
研究者番号: 9 0 3 3 3 9 4 7  
(H19→H20:連携研究者)  
萩田 真理子  
お茶の水女子大学・大学院人間文化創成科

学研究科・准教授  
研究者番号: 7 0 3 3 8 2 1 8  
(H19→H20:連携研究者)  
斎藤 秀司 (SAITO SHUJI)  
東京大学・大学院数理科学研究科・教授  
研究者番号: 5 0 1 5 3 8 0 4  
(H19→H20:連携研究者)  
辻 雄 (TSUJI TAKESHI)  
東京大学・大学院数理科学研究科・教授  
研究者番号: 4 0 2 5 2 5 3 0  
(H19→H20:連携研究者)  
森田 良幸 (MORITA YOSHIYUKI)  
広島大学・大学院理学研究科・助教  
研究者番号: 2 0 2 4 3 5 4 5  
(H20→H21:連携研究者)  
島田 伊知郎 (SHIMADA ICHIROU)  
広島大学・大学院理学研究科・教授  
研究者番号: 1 0 2 3 5 6 1 6  
(H21→H22:連携研究者)  
石井 亮 (ISHII AKIRA)  
広島大学・大学院理学研究科・准教授  
研究者番号: 1 0 2 5 2 4 2 0  
(H21→H22:連携研究者)  
山内 卓也 (YAMAUCHI TAKUYA)  
大阪府立大学・総合教育研究機構・教育拠点形成教員  
研究者番号: 9 0 4 3 2 7 0 7  
(H21→H22:連携研究者)  
志甫 淳 (SHIHO ATSUSHI)  
東京大学・大学院数理科学研究科・准教授  
研究者番号: 3 0 2 9 2 2 0 4  
  
(3)連携研究者  
斎藤 睦夫 (SAITO MUTSUO)  
広島大学・大学院理学研究科・助教  
研究者番号: 3 0 5 0 7 7 3 6  
原本 博史 (HARAMOTO HIROSHI)  
呉工業高等専門学校・一般科目・講師  
研究者番号: 4 0 5 1 1 3 2 4