

先端研究拠点事業
平成19年度 事業実績報告書

採用年度	平成18年度
種別	拠点形成型
分科細目	数学 代数学
採用番号	18005

平成20年 4月21日

独立行政法人 日本学術振興会理事長 殿

拠点機関代表者・氏名 学長・浅原 利正 職印

コーディネーター職・氏名 教授・松本 眞

領域・分野	数物系科学
分科細目名（分科細目コード）	代数学(4101)
採用番号	18005
研究交流課題名（和文）	数論幾何・モチーフ理論・ガロア理論の新展開と、その社会的実用
研究交流課題名（英文）	New Developments of Arithmetic Geometry, Motive, Galois Theory, and Their Practical Applications
採用期間	平成18年4月1日～平成20年3月31日（24ヶ月）

《実施組織体制》

日本側

拠点機関名	広島大学
実施組織代表者（職・氏名）	学長・浅原 利正
コーディネーター（職・氏名）	教授・松本 眞
協力機関数	3
参加者数	96名

相手国1

国名	アメリカ
拠点機関名	デューク大学
実施組織代表者（職・氏名）	
コーディネーター（職・氏名）	教授・Richard Hain
協力機関数	0
参加者数	7名

相手国 2

国名	イタリア
拠点機関名	パドバ大学
実施組織代表者（職・氏名）	
コーディネーター（職・氏名）	教授・Bruno Chiarellotto
協力機関数	0
参加者数	5名

相手国 3

国名	フランス
拠点機関名	パリ 11 大学 Orsay
実施組織代表者（職・氏名）	
コーディネーター（職・氏名）	教授・Jean-Marc Fontaine
協力機関数	1
参加者数	52名

交流目標の達成（見込）状況

① 平成19年度事業計画における達成目標

本研究交流の目的は、世界的規模での研究交流を通して、

1. 現代的純粋数学理論を発展させる、
 2. 古典から最先端までの純粋数学理論より、暗号・乱数など実用に供される技術のシードを抽出し・展開させ、実用プログラムを開発する、
 3. 社会的実用性の立場から数学に求められるものを、純粋数学者にフィードバックする、
- の3点にある。

H18年度に構築された国際的研究協力体制を元に、共同研究・セミナーなどを通して数論的代数幾何・モチーフ理論・ p 進幾何などの先端的純粋数学の研究交流を押しすすめ、暗号・乱数など実用に供される技術を開発し実際に社会に普及を図る。

大学院学生など若手研究者を中心に、海外の先端的研究者と交流する機会をつくり、さらに高度な実用理論に触れる機会を設け、研究協力拠点体制を構築する。

② 平成19年度事業計画の達成状況

A. 学術的な成果(代表的なものを抜粋)

純粋数学的成果:

名古屋大・古庄英和助教は、本事業による一部支援を受けて数論幾何において基本的な対象である「Grothendieck-Teichmüller 群」の構造を研究し、成果は数学学術雑誌の最高峰とも呼ばれる Annals of Math. に論文掲載予定となった。

Duke 大・Hain 教授と広島大学・松本教授はトレリ群から写像類群への自然な埋め込みが、相対 $pro-1$ 完備化後に単射性を失うことを示し、共著論文を投稿中である。

Padova 大・Chiarellotto 教授と広島大学・都築教授は p 進対数的増大度に関する「Dwork の問題」の正確な定式化と階数 2 の場合の証明を行い、共著論文を投稿中である。

パリ南大学・Caro 講師と都築教授は「数論的D加群における極大過剰決定系」の研究を行い、共著論文を投稿中である。

実用的成果:

モンリオール大学 L'Ecuyer 教授, Panneton 研究員と広島大学の松本教授、D3学生原本博史、山形大学西村助教は、従来は時間がかかって現実的ではなかった、メルセンヌツイスターなどの長周期疑似乱数のジャンプアルゴリズムを共同開発し、共著論文はOR分野では著名な Informs Journal of Computation 誌に受理された。

計算機の進化する並列性に呼応したデザインを持つ疑似乱数発生器 SIMD-oriented Fast Mersenne Twister(SFMT)を広島大学松本教授・斎藤睦夫研究員は共同開発し、論文は査読付き国際会議録に受理された。

B. 協力関係の基盤構築

国内で4回、イタリアで1回、フランスで1回の国際研究集会を共催し、米国・イタリア・フランス側研究者との研究協力体制を強化した。特に、18年度と同様に、「フランス・サマースクール」には若手の養成と若手同士の研究交流に重点をおき、博士課程学生を中心に11名の日本人参加者を補助した。

C. 若手育成

上記Bのほか、広島大学にて、博士課程学生および学振による海外 Fellowship による来日者らを主な発表者とする整数論集会を開催し、若手の研究成果発表ならびに交流の場を設けた。この集会では、暗号理論に応用される数論幾何の先端的研究について、この分野で著名な東工大・佐藤孝和准教授による特別講演も有り、若手の啓発を図った。

本事業参加メンバーである齋藤睦夫広島大学非常勤研究員(社会人学生として博士課程1年に在学中)は、上述の SFMT 乱数発生法、およびその暗号耐性化 CryptMT に関して3編の査読付き共著論文を発表し、広島大学理学研究科に助教として08年1月1日付けで採用された。広島大学山内卓也非常勤研究員は、本事業によりフランスのセミナーに派遣されるなどして整数論に関する研究成果を挙げ、大阪府立大学に任期付き助教として採用された。そのほか、広島大学D3学生の原本博史氏、北臺如法氏がそれぞれ広島大学特別研究員、広島大学特任助教という任期付きの有給のポジションに2008年4月1日より採用された。ほか、多くの若手研究者が学振PDや特別研究員などに採用された。

D. 情報収集整備

国際的共同研究・セミナーを通して、まだ論文に書かれていない最新の研究成果についての情報を収集することができた。また、広島大学が発行する国際学術雑誌 Hiroshima Mathematical Journal に対する投稿論文数が増えたほか、従来は比較的少なかった数論幾何分野からの投稿が増えたなど、情報の収集力が高まった。

E. 事業の波及効果

本年度の研究交流成果により、本事業の国際的知名度は高いものとなった。カナダ・モントリオール大学、およびフランス・レンヌ大学から、本事業の研究拠点になりたいという申し入れがあったほか、パリ第13大学から協力機関になりたいという申し入れがあった。本事業の実用的な成果の一つである SFMT 擬似乱数発生法のプログラムは広島大学ホームページで公開され、現在までに16000件を超えるダウンロードがあり、世界に広がりがつつある。また、乱数・アルゴリズム関係で、二つの国内企業から広島大学松本教授に共同研究開発の申し入れがあり、現在進行中となっている。

実施状況

研究交流計画実施にあたる実施体制

- ・米国側研究拠点 Duke 大学コーディネータ Hain 教授を松本教授は2007年8月9日から8月21日に訪問し、共同研究を遂行したほか、本事業の延長をにらんで米国NSFへの予算申請などの打ち合わせを行った。
- ・フランス側研究拠点パリ南大学コーディネータ Fontaine 教授と松本教授、協力機関東京大学齋藤毅教授とは電子メールで連絡をとりあい、フランス側予算確保の調整を行った。東京大学で齋藤毅教授らによりオルガナイズされた本事業共催セミナー「分岐と消失輪体」には、パリ南大学より Illusie 教授・Caro 講師、フランス側協力機関レンヌ大 Abbes 教授、米国研究協力者 Kedlaya 教授ら、多数の相手国側協力者、ならびに協力機関名古屋大学・京都大学から複数のメンバーが参加し、本事業の今後の進展についての話し合いをおこなった。この際、Abbes 教授からフランス・レンヌ大学を研究拠点に昇格することについての申し出が、パリ13大学 Mocrane 教授から同大学を協力機関に追加する申し出があった。
- ・イタリア側研究拠点パドバ大学コーディネータ Chiarellotto 教授は相手国側予算で広島大学を2008年3月に訪問、同大学都築教授との共同研究を進める傍ら、松本教授と本事業の次年度の計画について話し合った。

日本側拠点機関における研究交流課題への取り組み（事務支援体制等の観点より）

- ・本事業委託手数料にて、英語が堪能な事務処理担当非常勤職員を一名雇用し、本国際事業に関する数多の事務処理を行ってもらった。雇用に関しては、理学研究科事務および財務部が適切な処理を行った。
- ・広島大学国際部国際企画連携グループと、上記非常勤職員は、緊密な協力のもと、海外からのセミナー参加者の旅行事務をはじめとする多くの事務処理を効率的に行った。同グループは、学術振興会との連絡をスムーズに行い、かつ、「一般の方の視点」による本事業へのコメント・フィードバックを与えることにより、本事業の実施に大いに役立った。
- ・広島大学は学長裁量経費 80 万円を Hiroshima Mathematical Journal の電子化関連予算として計上し、本事業の情報収集発信能力向上に協力した。
- ・広島大学大学院理学研究科は、本事業を「理学研究科が特に重点を置く事業」の一つとして認定した。これにより、広島大学にて 5 名内部措置される「特別研究員（助教同等の給与）」にD3学生原本氏が応募可能となり、多数の応募の中から原本氏の 2008 年 4 月 1 日からの採用が決定した。

共同研究

1. 日本側コーディネータ松本眞教授を代表者とし、米国コーディネータ・デューク大学ヘイン教授、京都大学玉川安騎男教授・望月新一教授、名古屋大学古庄助教らをメンバーとする「ガロア群、写像類群とモジュライ空間の幾何」の共同研究。
ヘイン教授を松本教授は 2007 年 8 月に訪問、トレリ群の写像類群への埋め込み写像が、相対 pro-l 完備化後では埋め込みとならないという結果を証明し、共著論文を執筆し投稿した。松本教授は京都大学を訪問し、京都滞在中のフランス・パリ Jussieu 大学 Marco Boggi 研究員ならびに玉川・望月教授と上記の研究成果について研究討論を行った。
2. 研究拠点広島大学のメンバー都築暢夫教授を代表者とする、イタリアパドバ大学との共同研究「数論的微分方程式とその Frobenius 構造」。イタリア側ではキアレロット教授、バルダサーリ教授らがメンバーである。キアレロット－都築は p 進対数的増大度に関する Dwork の問題」の階数 2 の場合の証明を与える論文を執筆し、現在投稿中となった。キアレロット教授は 2008 年 3 月広島大学を訪問、一般の階数の場合についての解決を模索した。
3. 松本教授を代表者とし、研究協力者カナダ・モントリオール大学オペレーションリサーチ学科レキエ教授・広島大学齋藤睦夫研究員・山形大学理学部西村助教・お茶の水女子大学理学部萩田真理子准教授らをメンバーとする共同研究「高速多機能擬似乱数の開発」。2007 年 3 月にレキエ教授が広島を訪問し、研究討論を行い、その後電子メールにより共同研究を進めた。メルセンヌツイスタ擬似乱数発生法に対する高速ジャンプ技法（原本－松本－西村－レキエ－パネトンの共同研究、論文受理済み）、並列性を有効利用した SFMT 擬似乱数（齋藤－松本、論文掲載済み）、整数乗算の持つ準群性と非線形性を利用した CryptMT 暗号乱数（松本－齋藤－西村－萩田、論文掲載済み）といった成果を挙げている。

セミナー

1. 2007年6月「数論幾何における p 進的手法とその応用2007」(開催地:東京大学)
 p 進ホッジ理論を含む国際会議であり、広島大学都築教授・イタリア側拠点パドバ大学 Garuti 助手・フランス側拠点パリ第11大学 Caro 講師ら海外から6名の講演者があった。Caro 講師と都築教授は共同研究に着手した。
2. 2007年7月「モチーフ勉強会第3回」(開催地:東京大学)
モチーフの理論について、専門家によるサーベイ講演を含む若手を中心とした国内セミナーであった。協力機関の米国ガイサー助教授(2006年7月-2008年7月 東京大学客員研究員として本邦滞在中)を運営組織と講演者に加え、英語により行われる国際性の高いセミナーであり、若手研究者の先端的モチーフ理論の理解を深めた。
3. 2007年7月「セールのモジュラー性予想サマースクール」(開催地:フランス・ルミニ)
ガロア表現に関する大きな未解決予想であったセールのモジュラー性予想の Khare と Wintenberger による解決と、その周辺に関する先端的研究集会。パリ11大学 Jean-Marc Fontaine 教授他が主催、東大数理の斎藤毅教授らが講演。本事業により日本から11名参加し、若手同士の国際的研究交流を行った。
4. 2007年7月「第6回広島整数論集会」(開催地:広島大学)
6回を迎える国内整数論集会であり、若手研究者の得た知見を集積するとともに、純粋研究系の研究者へ実用の視点をフィードバックするため、協力研究者東工大・佐藤孝和准教授による「暗号理論への数論幾何の利用の現在」についての特別講演を行った。
5. 2007年9月「分岐と消失輪体」(開催地:東京大学)
数論幾何学の最先端である分岐理論、消失輪体、リジッド幾何、 p 進幾何について、東京大学斎藤毅教授らがオルガナイザーとなり、研究集会を行った。フランス側拠点イルージュ教授、協力機関フランスレンヌ大学ベルテロ教授ら、世界的研究者が多数参加した。本会議における懇親会では、学術振興会より丹生課長らのご来臨され、本事業に対する賞賛と励ましの言葉をいただいた。この懇親会にて、多数の諸外国研究者と本事業についての打ち合わせを行い、レンヌ大学からは研究拠点への昇格について、パリ11大学からは協力機関としての参加についての相談があったほか、ドイツほか多くの国の研究者から本事業についての問い合わせがあった。
6. 2007年10月「数論的代数幾何会議」(開催地:イタリア セトラロ)
欧州EUの研究教育ネットワーク「数論的代数幾何」の最終年度における総括的な研究集会である。主催はイタリア研究拠点パドバ大学のキアレロット教授ら。協力機関名古屋大学の古庄助教が招待講演を行ったほか、協力機関京都大学加藤文元准教授らが参加し、今後の本事業の展開について打ち合わせがなされた。

研究者交流

前年度の研究者交流によって得られた研究成果を発表するために、東京大学齋藤秀司教授、広島大学松本 眞教授、木村俊一准教授、原本博史博士学生、齋藤睦夫研究員、須川敏幸准教授、石井亮准教授らを研究集会に派遣し研究発表、ならびに共同研究の模索を行った。

齋藤秀司はドイツレーゲンスブルグ大学を訪問し、本事業研究協力者ヤンセン教授・シュミット教授(2007年に東大・京大・広島大を訪問)とモチーフ的コホモロジーについての研究成果発表ならびに研究討論を行った。ドイツは将来的に本事業の相手国とすることを検討しているが、本事業の規模との兼ね合いを模索中である。

木村俊一准教授は本事業研究成果であるモチーフの有限次元性について、パリ11大学にて研究発表を行った。

齋藤睦夫研究員は、カナダ・オタワで開催された Selected Area in Cryptography2007 に参加し、CryptMT Ver.3に関する研究発表を行った。この成果は査読付き国際会議録に収録済みである。

若手では、協力機関京都大学D2学生森田和真氏、筑波大学木村健一郎助教をパリ第11大学に研究交流目的で派遣した。それぞれ p 進ホッジ理論・代数的サイクルの理論に関して研究成果をあげている。

そのほか、広島大・東大・京大・名古屋大を中心に、国内での研究連絡を密接におこない、国際交流を意義深いものにさせる準備とした。