様式19 別紙1

課題番号	GR 087

先端研究助成基金助成金(最先端・次世代研究開発支援プログラム)
実施状況報告書(平成 24 年度)

本様式の内容は一般に公表されます

研究課題名	高次元 p 進ディオファントス近似と整数格子クリプトシステム
研究機関・ 部局・職名	日本大学・理工学部・教授
氏名	平田典子 (河野典子)

1. 当該年度の研究目的

当該年度である平成24年度の主要研究目的は以下であった.

(1) p進楕円対数の一般n個の一次結合のディオファントス近似不等式の構築とその応用.

(2) (1)の近似の手法を, 回帰数列を底とするディオファントス方程式に適用し, 整数解を決定する.

(3) (1)のp進楕円対数一般化に相当するp進楕円多重対数関数および楕円版ではないp進多重対数関数に対し収束半径内の有理数における値の数論的性質を求める.

(4) 楕円曲線の整数点を応用した新しい暗号を定義する写像を与えるための条件を考究して, 平成25年度にクリプトシステムを構築する準備を行う。

2. 研究の実施状況

(1) 研究目的(1)「p進楕円対数の一般n個の一次結合のディオファントス近似不等式」については, 完全な証明が遂に完成した. 非常に長く極めて大がかりな証明である. 現在は定理の主張だけを, URL
http://trout.math.cst.nihon-u.ac.jp/~hirata/publications.html
に掲載している状態であるが, 証明の最終チェック終了後に急いで投稿する. なおこの主張は, 短期的な成果ではなく, 絶対的な結果として将来にわたり長期間に使われ続けるような基礎的なものであり, 他の様々な科学技術分野にも応用され得るような数理科学の結果として, 国際的にも息の長いものになる自負がある.

(2) 研究目的(2)「回帰数列を底とするディオファントス方程式」については目標通りの成果が得られた. 一部を既に F. Lucaと共同でまとめ, Rocky Mountain Journal of Mathematics に投稿して掲載決定となった (ただし研究・査読・印刷に長時間かかる基礎科学である数学の常ではあろうが, 掲載決定済の当該論文の掲載される巻の印刷は2年以上も後になるということである). 雑誌論文の「未掲載」欄の(1)がその成果である. 更なる進展を目指し現在も研究を継続している,

(3) 研究目的(3)「p進多重対数関数に対する数論的性質」についても複数の結果が得られ, 国内外で既に口頭発表を行った. 会議発表の専門家向けの欄の(1)(2)(3)(4)(5)である. 実際には研究開始当初の予想を遥かに超えた良い結果が得られたので, 発表の際における専門家からの反響も手応えのあるものであった. これは, 雑誌論文の「掲載済み-査読あり」の欄に記載の論文(2)の発展および, 「掲載済み-査読なし」の欄に記載の論文(1)の発展に相当する. 証明を現在まとめており, 近々投稿する予定である.

様式19 別紙1

(4) 研究目的(4)「楕円曲線の整数点を応用した新しい暗号構築準備」については, A. Pethoと共同で研究を進めていたが, 暗号への具体的応用を構築するための最初の成果が得られたので, 2013年6月25日から28日までチェコ Telc で開かれる予定の暗号の国際研究集会 Central European Conference on Cryptology 2013 にて, 共同研究者 A. Pethoが発表する. 発表についての事前審査をパスして, 口頭発表論文アブストラクトとして採択され, プログラムにも記載されている. 研究集会プログラムURL :
http://www.fi.muni.cz/cecc/
この内容は著者:N. Hirata-Kohno and Attila Petho,
題名:On a key exchange protocol of a cryptosystem based on Diophantine equations の論文として
この研究集会のプロシーディングスに投稿予定である.
(5) ディオファントス近似の応用として整数格子に関する別の知見も得られたため, 論文を情報系の雑誌 Interdisciplinary Information Sciencesに投稿し, 掲載決定の通知を得た. 雑誌論文の「未掲載」欄の論文(2)である. この発展については, 雇用中のRAとも共同で考察しており, 25年度に完成させる予定である.
(6) 数学の場合, 国民との科学・技術対話としては, 例えば中学生や高校生相手に, 思いがけないような数学の応用を解説した平易な講演をすることが歓迎される. この当該研究課題の応用として得られた無理数の話題について内容をまとめた数学教育の口頭発表などを, 国民との科学・技術対話の一環としておこなった.

3. 研究発表等

雑誌論文 計 5 件	(掲載済み－査読有り) 計 2 件 (1) 平田典子, Diophantus 近似, 岩波書店「数学」(日本数学会誌), 64巻, (2012), 254--277. (2) N. HIRATA-Kohno and H. Okada, A note on linear independence of polylogarithms over the rationals, Proceedings of the Japan Academy, series A, 88,(2012), 156--161 (DOI: 10.3792/pjaa.88.156). (掲載済み－査読無し) 計 1 件 (1) N. HIRATA-Kohno , Arithmetic properties of p-adic elliptic polylogarithms and irrationality, Diophantische Approximationen, Oberwolfach Report Vol. 9, Issue 2, 1347--1351, (2012), eds. Y. Bugeaud and Yu. V. Nesterenko, European Math. Society (DOI: 10.4171/OWR/2012/22). (未掲載) 計 2 件 (1) N. HIRATA-Kohno and F. Luca, On the Diophantine equation F_n^x + F_{n+1}^x = F_m^y, Rocky Mountain Journal of Mathematics, accepted for publication (査読有り, 掲載決定). (2) Masaru Ito and Noriko Hirata-Kohno, Optimization for lattices and Diophantine approximations, Interdisciplinary Information Sciences, accepted for publication (査読有り, 掲載決定).
会議発表 計 7 件	専門家向け 計 5 件 (1) N. HIRATA-Kohno, Arithmetic properties of p-adic elliptic polylogarithms and irrationality, Oberwolfach MFO, Diophantische Approximationen Workshop, Germany, 2012, April 27. (2) N. HIRATA-Kohno, Polylogarithms revisited from the viewpoint of the irrationality, Algebraic Number Theory and Related Topics, The Research Institute for Math. Science Workshop, Kyoto University, 2012, December 07.

	(3) N. HIRATA-Kohno, Sur l'irrationalite de polylogarithmes, Seminaire de Theorie des Nombres, University of Caen, France, 2013, February 28. (4) N. HIRATA-Kohno, L'irrationalite_ de polylogarithmes p-adique, Problemes Diophantiens, University of Paris 6, Groupes d'Etudes sur les Problemes Diophantiens, Institut de Mathematiques de Jussieu, University of Paris 6 (Jussieu Campus), France, 2013, March 7. (5) N. HIRATA-Kohno, Sur l'irrationalite de polylogarithmes, Seminaire Arithmetique et geometrie algebrique, Institut de Recherches Mathematique Avancee, University of Strasbourg, France, 2013, March 8. 一般向け 計 2 件 (1) 平田典子, 楕円多重対数関数とその数論的性質, 大阪大学大学院理学研究科数学専攻談話会, 2012, May 14. (2) 平田典子, 多重対数関数とその値の数論的性質, 東北大学大学院理学研究科数学専攻談話会, 2012, October 15.
図 書 計 0 件	
産業財産権 出願・ 取得状況 計 0 件	(取得済み) 計 0 件 (出願中) 計 0 件
Web ページ (URL)	http://trout.math.cst.nihon-u.ac.jp/~hirata/Next.html
国民との科学・技術対話の実施状況	(1) 平田典子,「ビー玉で遊ぶと現れる整数格子の最先端研究」, 日本大学理工学部駿河台入試フォーラム, 対象 高校生, 参加者数 約90名, 2012年7月15日. (2) 平田典子,「方眼紙で考える分数のはなし」, 藤岡市おもしろ数学教室(群馬県藤岡市教育委員会主催, 日本数学会後援), 対象 中学生, 参加者数 約150名, 2012年10月24日 http://www.city.fujioka.gunma.jp/kakuka/f_syougai/kennsyoujigyou.html (3) 平田典子,「三角比と正多角形」, 日本大学豊山女子高等学校 理数科講座, 対象 高校2年生, 参加者数 35名, 2012年12月14日 http://www.buzan-joshi.hs.nihon-u.ac.jp/life/121214.html (4) Y. Washio, H. Okada and N. Hirata-Kohno,「三角比と無理数を関連づける数学の視覚的教材の提案:正弦の値の性質と正多角形の頂点配置問題」(講演 2012年8月24日),日本工学教育協会 平成24年度工学・工学教育研究講演会(芝浦工業大学豊州キャンパス)第60回工学・工学教育研究講演会講演論文集, 560-561. (5) N. Hirata-Kohno and Y. Washio,「単位円上の有理数座標の点の幾何学的考察」(2012年9月20日),秋季数学教育学会 平成24年度講演会(九州大学伊都キャンパス)数学教育学会誌臨時増刊号 2012年秋季例会発表論文集, 84-86.
新聞・一般雑誌等掲載 計 1 件	(1) 河野(平田)典子,・鷲尾勇介, 整数格子を活用した三角比の視覚的教材と数学教育の実践研究, 工学教育 2013 年 5 月号 61 巻, No. 3, 113-115 (査読有り).
その他	なし

4. その他特記事項

なし.

様式19 別紙2

課題番号	GR087

実施状況報告書(平成24年度) 助成金の執行状況

本様式の内容は一般に公表されます

1. 助成金の受領状況(累計) (単位:円)

	①交付決定額	②既受領額(前年度迄の累計)	③当該年度受領額	④(=①−②−③)未受領額	既返還額(前年度迄の累計)
直接経費	15,000,000	5,800,000	5,000,000	4,200,000	0
間接経費	4,500,000	1,740,000	1,500,000	1,260,000	0
合計	19,500,000	7,540,000	6,500,000	5,460,000	0

2. 当該年度の収支状況 (単位:円)

	①前年度未執行額	②当該年度受領額	③当該年度受取利息等額(未収利息を除く)	④(=①+②+③)当該年度合計収入	⑤当該年度執行額	⑥(=④−⑤)当該年度未執行額	当該年度返還額
直接経費	54,900	5,000,000	0	5,054,900	5,000,000	54,900	0
間接経費	0	1,500,000	0	1,500,000	1,500,000	0	0
合計	54,900	6,500,000	0	6,554,900	6,500,000	54,900	0

3. 当該年度の執行額内訳 (単位:円)

	金額	備考
物品費	2,609,090	計算用パーソナルコンピュータ、数学資料等
旅費	462,360	研究成果発表旅費(ドイツ)、研究討議参加旅費(Cean大学)等
謝金・人件費等	1,893,500	PD人件費、臨時職員人件費、専門知識提供に対する謝金
その他	35,050	研究連絡郵送料等
直接経費計	5,000,000	
間接経費計	1,500,000	
合計	6,500,000	

4. 当該年度の主な購入物品(1品又は1組若しくは1式の価格が50万円以上のもの)

物品名	仕様・型・性能等	数量	単価(単位:円)	金額(単位:円)	納入年月日	設置研究機関名
				0		
				0		
				0		