

## 科学研究費助成事業 研究成果報告書

平成 27 年 5 月 29 日現在

機関番号：17401

研究種目：基盤研究(C)

研究期間：2012～2014

課題番号：24540180

研究課題名(和文)非線形偏微分方程式系における解軌道のP進解析による複雑性構造解析

研究課題名(英文)Complexity structure analysis on the orbits of solutions of nonlinear partial differential equations by p-adic analysis

研究代表者

内藤 幸一郎 (NAITO, Koichiro)

熊本大学・自然科学研究科・教授

研究者番号：10164104

交付決定額(研究期間全体)：(直接経費) 4,000,000円

研究成果の概要(和文)：多次元p-進近似格子による多重p-進無理数有理近似解析の研究を行い、p-進弱Liouville数を振動数としてもつ多重準周期力学系の離散軌道の再帰性について解析し、軌道が予測不能性を持つことを示した。p-進展開の係数からなる記号列から構成される記号力学系の解析を行い、この力学系の再帰的次元と位相的エントロピーとの間に成立する不等式を導いた。

p-進近似格子における最小ベクトル問題(SVP)について、多重p-進無理数有理近似問題(SAP)から得られる理論値とLLLアルゴリズムを用いた実験値との比較検証を行った。これらの実験結果を元に、p-進近似格子のSAP解を秘密鍵とする暗号系の提案を行った。

研究成果の概要(英文)：Analyzing simultaneous rational approximations of irrational p-adic numbers by using multi-dimensional p-adic approximation lattices, we investigate some recurrent properties of discrete orbits given by quasi-periodic dynamical systems, the frequencies of which are weak Liouville p-adic numbers and we show some unpredictability properties of the orbits. For the symbolic dynamical systems given by the coefficient sequences of expansions of p-adic numbers we give some inequality relations between the recurrent dimensions and the topological entropy of these systems.

For the shortest vector problems of p-adic approximation lattices we compare the theoretical solutions given by the simultaneous approximation problems (SAP) and the numerical solutions estimated by the LLL algorithm. By using these results we propose a new lattice based cryptosystem, the private keys of which are the SAP solutions of p-adic lattices.

研究分野：基礎解析

キーワード：P-進数論 格子理論 暗号理論 力学系 非線形偏微分方程式

## 1. 研究開始当初の背景

提唱されてからすでに 100 年以上の歴史をもつ  $p$ -進数体  $\mathbb{Q}_p$  (K.Hensel, 1902) は、フェルマーの定理の証明でも本質的に利用されたように (A.Wiles, 1995)、数論などの代数学の分野では極めて常識的な概念である。一方、連続的な実数体を基礎とする解析分野では非連結な  $\mathbb{Q}_p$  はこれまでほとんど注目されることはなかった。しかしながら近年、超弦理論など、プランクスケールレベルの時空間の本質的な構造にまで深く関わる理論物理学の分野では、時空間の本質的な構造は非アルキメデス的であるという観点から、非アルキメデス距離空間である  $\mathbb{Q}_p$  を基礎とする  $p$ -進解析を利用する研究が極めて盛んに行われ成果を上げている (V.S.Vladimirov, 1994)。数理解析分野、特に関数方程式分野では  $p$ -進数体  $\mathbb{Q}_p$  を基礎とする解析はこれまでほとんど行われていなかったが、爆発や乱流などのより複雑な非線形現象を解析するにあたり、 $p$ -進解析の理論は斬新な手法を与える可能性があり、フーリエ解析や作用素論など関数方程式の基礎理論分野ではこれらの数論の概念を導入した解析理論の展開、拡張が行われ始めている (A.N.Kochubei, 2001, S.Albeverio, et.al., 2010)。

これまでの代表者の研究では連分数展開をはじめとする数論的解析とアトラクター解などの解軌道の挙動解析、特に再帰性解析との関連を明らかにすることを主題としている。離散的軌道に対して上と下の再帰的次元を軌道の  $\varepsilon$  近傍への再帰時間を利用して、それぞれ、 $\varepsilon \rightarrow 0$  の上極限、下極限により定義し、上極限と下極限の差を次元の GAP として定義した。この GAP の値が正のときには再帰時間の不定性が現れると理解されるため、GAP 値を軌道の予測不能性を表す指標として提案している。また、一般的な記号力学系において位相的エントロピーの値が上と下の再帰的次元の間に挟まれる不等式を示した。この不等式から、下の再帰的次元が正であればエントロピーが正、つまり系がカオス的となることが導かれるので、カオス性と再帰性の関連を明示する強力な道具立てを得ている。

## 2. 研究の目的

本研究では、上述の代表者等による基礎研究に  $p$ -進数論を取り入れた  $p$ -進解析理論の構築を目指すとともに、非線形偏微分方程式系に現れる複雑解の数理解析にこの  $p$ -進解析の理論を応用することを目的としている。

## 3. 研究の方法

$p$ -進解析は数論と解析の境界複合領域にある理論であり、解析分野の研究者の研究結果や著述はまだ僅かであるが、理論物理や数理解析分野の研究者の研究は盛んに行われている。数論的な解析理論の拡張とその数理解析分野への応用、特に非線形偏微分方程式系であらわされるモデルへの応用研究とを並行して行った。

数論を含む代数分野の研究については分担者城本氏の協力のもとに行い、理論解析だけでなく、とくに複雑性の著しい暗号理論の分野への  $p$ -進解析の応用も視野に入れての研究を展開した。特に、代表者等はオープンソース数式処理ソフト Sage を導入し、安全性検証などの暗号理論研究に必須となる計算機支援実験解析を理論解析と並行して行った。また、 $p$ -進解析における数論に関わる理論研究を行う際には「準周期タイリング」の研究者グループとの定期的開催される研究会などを通して最新研究情報交流を行っている。

代表者と分担者和田氏、三沢氏は、非線形シュレディンガー方程式を始めとする様々な非線形偏微分方程式に対して、その解の挙動についての複雑性解析を行った。カオス的な複雑状態にあることが予想される爆発解や複雑なフラクタル構造性が予想される自己相似解などをもつ非線形偏微分方程式についても、代表者と分担者等が世話人として定期的に参加している「熊本大学応用解析セミナー」で、非線形偏微分方程式に関する最新の研究情報交流を行い、研究展開を行った。

## 4. 研究成果

(1) 平成 24 年度では  $p$ -進解析理論の研究とその数理解析分野への応用を目的としていたため、非線形偏微分方程式理論の数学的基礎である関数解析と  $p$ -進数論を融合した  $p$ -進関数解析学についての研究を進めた。特に、 $p$ -進シュレディンガー作用素のスペクトルについての解析研究では、ポテンシャルに対するシフト変換や拡大変換における固有値の不変性についての結果が得られた。また、代表者は  $p$ -進数の連分数展開について  $p$ -進近似格子理論を利用した解析研究を行い、 $p$ -進弱 Liouville 条件の下で最小ノルムベクトルが求められること、すなわち最良近似が得られることを示した。以上の研究結果については、国際研究会 NAO-Asia2012 での招待講演及び複数の一般講演を通して発表した。詳細な研究内容については同 Proceedings に掲載された。

$p$ -進作用素解析では分数冪作用素、分数冪関数空間の研究が必須である。分担者和田氏は、分数冪関数空間におけるシュレディンガー作用素の詳細な解析研究を行い、複数の学術雑誌にこれらの研究成果を発表している。分担者三沢氏は  $p$ -ラプラス型作用素をもつ非線形放物型方程式の解が分数冪型の連続性であるヘルダー連続性をもつことを示し、学術雑誌 J. Diff. Eq. に発表した。

本研究では複雑性の著しい暗号理論の分野への  $p$ -進解析の応用研究も目指している。この基礎研究として統合数式処理ソフトウェア SAGE を利用した数値解析研究を行い、 $p$ -進無理数を実装する研究を通して、 $p$ -進 Liouville 数の指数評価についての数値解析を行った。これらの研究結果は京都大学数理解析研究所研究会「非線形解析学と凸解析

学の研究」で講演発表を行い、同講究録に掲載された。分担者城本氏は、これらの暗号理論の基礎的研究となる符号理論についての研究結果を組み合わせ論の国際研究集会での講演、学術雑誌で発表した。

(2)平成 25 年度では、代表者は多次元  $p$ -進近似格子を利用した多重  $p$ -進無理数有理近似解析の研究を行い、多重近似指数と  $p$ -進弱 Liouville 型無理数の有理近似指数との間に成立する不等式関係を導出した。さらに、 $p$ -進弱 Liouville 型無理数の冪を振動数としてもつ多重準周期力学系の離散軌道の再帰性について解析し、再帰的次元の GAP 値が正の値を取ることを導くことにより、軌道が予測不能性を持つことを示した。これらの研究結果については、国際学会 NACA2013 で招待講演発表を行い、さらにその詳細は学術雑誌 *P-adic Numbers Ultrametric Anal. Appl.* に掲載された。

代表者は暗号理論の安全性の基礎となる NP 困難性をもつ最小ベクトル問題 SVP を  $p$ -進近似格子において解析し、多重  $p$ -進無理数有理近似理論から得られる理論値と、SVP の近似解法である LLL アルゴリズムによる実験値との比較検証を行った。100 未満の多重次元では LLL が理論値に近い最小ベクトルを導出する有力なアルゴリズムであることが示された。実用化された格子暗号系としては NTRU 暗号が知られているが、本研究では、NTRU 暗号の高速化を目的とした暗号システムを提案し、高速性と安全性に関わる数値実験検証を行った。これらの結果については NACA2013 での複数の一般講演で発表を行い、同 Proceedings に掲載されている。

本研究に関連して、分担者三沢氏は  $p$ -ラプシアン型偏微分方程式の定性解析についての研究結果を *J. Diff. Eq.* に複数論文発表し、分担者和田氏は非線形シュレディンガー方程式の分数冪解について *Proc. NAO 2012* に論文発表、同マクスウェル型方程式について数学会特別講演で発表した。分担者城本氏は符号理論の研究結果を *Designs Codes Crypt.* に論文発表、組み合わせ論の国際学会で招待講演発表を行った。

(3)平成 26 年度には、代表者は  $p$ -進展開の係数からなる記号列から構成される記号力学系の解析を行い、この力学系の再帰的次元と位相的エントロピーとの間に成立する不等式を導いた。 $p$ -進展開列が Sturm 列で、その回転指数が Liouville 数の場合には再帰的次元の GAP 値が正となり、軌道が予測不能性を持つことを示した。これらの結果は、ICM Satellite Conf. 2014 : NAO-2014 での招待講演で発表し、詳細は学術雑誌 *P-adic Numbers Ultrametric Anal. Appl.* に掲載された。

代表者は  $p$ -進近似格子における最小ベクトル問題 (SVP) について、多重  $p$ -進無理数有理近似問題 (SAP) から得られる理論値と LLL アルゴリズムを用いた実験値との比較検証を行った。これらの実験結果を元に、SAP

解を秘密鍵とする暗号系の提案を行った。これらの結果は、国際学会 NAO2014 で講演発表を行い、同会議論文誌に掲載予定である。また、関連した研究結果を The International Workshop on Nonlinear Analysis and Convex Analysis での招待講演発表、京都大学数理解析研究所研究集会「準結晶の数学的モデルとその周辺」で講演発表を行った。さらに  $p$ -進ナップザック暗号の提案を国内学会「暗号と情報セキュリティシンポジウム 2015」で講演発表を通して行った。

本研究に関連して、分担者三沢氏は  $p$ -ラプシアンを含む偏微分方程式の定性解析結果を *J. Diff. Eq.* に発表し、分担者城本氏は符号理論に関わる結果を *Linear Algebra Appl.* に論文発表し、組み合わせ論の国際学会で基調講演発表を行った。

#### 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 28 件)

- ① H. Inoue, S. Kamada, K. Naito, Simultaneous approximations of  $p$ -adic numbers and their applications to cryptography, *Proc. 4<sup>th</sup> Asian Conf. on Nonlinear Anal. Optim.*, 2015 in press, 査読有.
- ② H. Inoue, S. Kamada, K. Naito, Transference principle on simultaneous approximation problems of  $p$ -adic numbers and multidimensional  $p$ -adic approximation lattices, *Proc. 4<sup>th</sup> Asian Conf. on Nonlinear Anal. Optim.*, 2015 in press, 査読有.
- ③ H. Inoue, K. Naito, Entropy and recurrent dimensions of discrete dynamical systems given by  $p$ -adic expansions, *p-Adic Numbers, Ultrametric Analysis and Applications* 7, 2015, 147-157, 査読有, DOI: 10.1134/S2070046615020077
- ④ H. Inoue, K. Naito, Y. Yamada, Lattice reduction algorithms and their cryptographic applications, *Proc. 8th International Conference on Nonlinear Anal. Convex Anal.*, 2015, 167-176, 査読有.
- ⑤ H. Inoue, K. Naito, Simultaneous rational approximations of a  $p$ -adic number and its powers by  $p$ -adic approximation lattices, *Proc. 8th International Conference on Nonlinear Anal. Convex Anal.*, 2015, 155-166, 査読有.
- ⑥ M. Shi, K. Shiromoto, P. Sole, A note on a basic exact sequence for the Lee and Euclidean weights of linear codes over  $Z_l$ , *Linear Algebra and its Applications*, 2015 in press, 査読有,

- DOI:10.1016/j.laa.2015.01.033
- ⑦ T. Britz, K. Shiromoto, T. Westerback, Demi-matroids from codes over finite Frobenius rings, *Designs, Codes, and Cryptography* 75, 2015, 97-107, 査読有, DOI: 10.1007/s10623-013-9895-3.
- ⑧ C. Karim, M. Misawa, Hölder regularity for singular parabolic systems of p-Laplacian type, *J. Differential Equations*, 2015 in press, 査読有.
- ⑨ H. Inoue, K. Naito, Recurrent properties of quasi-periodic dynamical systems with multiple frequencies of p-adic Liouville numbers, *p-Adic Numbers, Ultrametric Analysis and Applications* 6, 2014, 195-206, 査読有.
- ⑩ H. Inoue, K. Naito, Simultaneous rational approximations of p-adic numbers by the LLL lattice basis reduction algorithm, *京都大学数理解析研究所講究* 1923, 2014, 163-171, 査読無.
- ⑪ K. Shiromoto, On critical exponents of matroids and linear codes, *京都大学数理解析研究所講究録* 1889, 2014, 7-12, 査読無.
- ⑫ M. Tanaka, T. Sogabe, K. Shiromoto, T. S. Usuda, Group covariance and formula of channel matrix of coded 4PSK signals by linear codes over  $F_4$ , *Proc. Int. Symp. Information Theory and Appl.* 2014, 348, 査読有.
- ⑬ T. S. Usuda, T. Sogabe, K. Shiromoto, Formula of channel matrix for covariant signal set with respect to a direct product of groups, *Proc. 12th Int. Conf. on Quantum Communication, Measurement and Computing*, 2014, 45, 査読有.
- ⑭ C. Leone, M. Misawa, A. Verde, The regularity for nonlinear parabolic systems of p-Laplacian type with critical growth, *J. Differential Equations* 256, 2014, 2807-2845, 査読有, DOI: 10.1016/j.jde.2014.01.018.
- ⑮ H. Inoue, K. Naito, Unpredictability of quasi-periodic dynamical systems with frequency of p-adic Liouville type numbers, *京都大学数理解析研究所講究* 1841, 2013, 8-16, 査読無
- ⑯ H. Inoue, K. Naito, p-adic continued fractons and a p-adic behavior of quasi-periodic dynamical systems, *Proc. 3rd Asian Conference on Nonlinear Analysis and Optimization* 3, 2013, 101-114, 査読有.
- ⑰ T. Murakami, K. Naito, Spectral analysis of p-adic fractional differential operators and p-adic Schrödinger type operators, *Proc. 3rd Asian Conference on Nonlinear Analysis and Optimization* 3, 2013, 219-232, 査読有.
- ⑱ K. Naito, Predictability and unpredictability of quasi-periodic dynamical systems, *京都大学数理解析研究所講究* 1821, 2013, 33-39, 査読無.
- ⑲ H. Uchizono and T. Wada, On well-posedness for nonlinear Schrödinger equations in fractional order Sobolev spaces, *Proc. 3rd Asian Conference on Nonlinear Analysis and Optimization* 3, 2013, 365-368, 査読有.
- ⑳ Y. Ishikawa, K. Shiromoto and T. S. Usu, Formula for the channel matrix of a certain class of  $(G, \chi)$ -covariant signals, *13th Asian Quantum Information Science Conference, Chennai, India, Extended Abstracts of AQIS2013*, 2013, 209-210, 査読有.
- ㉑ M. Misawa, A Hölder estimate for nonlinear parabolic systems of p-Laplacian type, *J. Differential Equations* 254, 2013, 847-878, 査読有.
- ㉒ T. Kobayashi, M. Misawa, L2-boundedness for the 2D exterior problems for the semilinear heat and dissipative wave equations, *RIMS Kokyuroku Bessatsu B42*, 2013, 1-11, 査読無.
- ㉓ T. Wada, Smoothing effects for Schrödinger equations with electro-magnetic potentials and applications to the Maxwell-Schrodinger Equations, *Journal of Functional Analysis* 263, 2012, 1-24, 査読有, DOI: 10.1016/j.jfa.2012.04.010
- ㉔ T. Wada, Continuous dependence for nonlinear Schrödinger equation in  $H^s$ , *Journal of Mathematical Sciences, University of Tokyo* 19, 2012, 57-68, 査読有.
- ㉕ H. Uchizono and T. Wada, On well-posedness for nonlinear Schrödinger equations with power nonlinearity in fractional order Sobolev spaces, *Journal of Mathematical Analysis and Applications* 305, 2012, 56-62, 査読有

DOI:10.1016/j.jmaa.2012.04.079

- ⑫ T. Britz, T. Johnsen, D. Mayhew, K. Shiromoto,  
Wei-type duality theorems for matroids,  
Designs, Codes and Cryptography 62, 2012, 331-341, 査読有,  
DOI: 10.1007/s10623-011-9524-y
- ⑬ C. Leone, M. Misawa, A. Verde,  
A global existence result for the heat flow of higher dimensional H-systems,  
J. Math. Pures Appl. 97, 2012, 282-294, 査読有,  
DOI: 10.1016/j.matpur.2011.11.001
- ⑭ M. Misawa, N. Nakauchi,  
Hölder continuity of minimizing symphonic maps, Nonlinear Anal. 75, 2012, 5971-5974, 査読有,  
DOI: 10.1016/j.na.2012.06.010

[学会発表] (計 31 件)

- ① H. Inoue, S. Kamada, K. Naito,  
Inhomogeneous simultaneous approximations of p-adic numbers and their applications to cryptography,  
ICM Satellite Conf. 2014: The 4<sup>th</sup> Asian Conference on Nonlinear Anal. Optim., 2014. 8. 8, Taiwan Normal University, Taipei, Taiwan.
- ② H. Inoue, S. Kamada, K. Naito,  
Transference Principle of Simultaneous approximation problems and LLL algorithm of multidimensional p-adic approximation lattices,  
ICM Satellite Conf. 2014: The 4<sup>th</sup> Asian Conference on Nonlinear Anal. Optim., 2014. 8. 8, Taiwan Normal University, Taipei, Taiwan.
- ③ H. Inoue, K. Naito,  
Entropy and recurrent dimensions of discrete quasi-periodic dynamical systems given by p-adic expansions,  
ICM Satellite Conf. 2014: The 4<sup>th</sup> Asian Conference on Nonlinear Anal. Optim., 2014. 8. 8, Taiwan Normal University, Taipei, Taiwan (招待講演).
- ④ H. Inoue, K. Naito,  
Shortest vector problems in p-adic lattices and simultaneous approximation problems of p-adic numbers,  
ICM Satellite Conf. 2014: The 4<sup>th</sup> Asian Conference on Nonlinear Anal. Optim., 2014. 8. 8, Taiwan Normal University, Taipei, Taiwan.
- ⑤ H. Inoue, K. Naito,  
The shortest vector problems in p-adic approximation lattices and their applications to cryptography,  
Int. Workshop on Nonlinear Anal. Convex Anal., 2014. 8. 19, Kyoto University, Kyoto (招待講演)
- ⑥ H. Inoue, K. Naito,  
Simultaneous approximation problems of p-adic numbers and their applications to cryptography,  
京都大学数理解析研究所共同研究研究集会「準結晶の数学的モデルとその周辺」, 2014. 10. 29, 京都大学数理解析研究所, 京都.
- ⑦ 井上裕仁, 内藤幸一郎,  
多次元 p 進近似格子と暗号理論への応用, 2015 年暗号と情報セキュリティシンポジウム, 2015.1.22, リーガロイヤルホテル小倉, 北九州.
- ⑧ K. Shiromoto,  
On the covering dimensions of a linear code and its relation to matroids,  
38th Australasian Conference on Combinatorial Mathematics and Combinatorial Computing, 2014. 12. 2, Victoria University of Wellington, Wellington, New Zealand.
- ⑨ M. Misawa,  
Regularity for the p-harmonic map heat flows,  
9th East Asia Partial Differential Equations Conference 2014. 7. 28, ホテル日航奈良, 奈良 (招待講演).
- ⑩ M. Misawa,  
Monotonicity type estimate and regularity of the p-harmonic map heat flows, 台湾数学会, 関数方程式分科会, 2014. 12. 6 (招待講演).
- ⑪ H. Inoue, K. Naito,  
Simultaneous rational approximations of a p-adic number and its powers by p-adic approximation lattices,  
8th international conference on NACA 2013, 2013. 8. 3, Hirosaki University, Hirosaki (招待講演).
- ⑫ K. Naito,  
Simultaneous rational approximations to p-adic numbers and the theory of lattices,  
8th international conference on NACA 2013, 2013. 8. 3, Hirosaki University, Hirosaki.
- ⑬ H. Inoue, K. Naito, Y. Yamada,  
Reduction algorithms for p-adic approximation lattices and their cryptographic applications,  
8th international conference on NACA 2013, 2013. 8. 3, Hirosaki University, Hirosaki.
- ⑭ H. Inoue, K. Naito,  
Simultaneous rational approximations of p-adic numbers by the LLL lattice basis reduction algorithm,

京都大学数理解析研究所研究集会「非線形解析学と凸解析学の研究」, 2013. 10. 10, 京都大学数理解析研究所, 京都 (招待講演) .

- ⑮ 和田 健志,  
平滑化効果と Maxwell-Schrödinger 方程式の大域的適切性,  
日本数学会年会特別講演, 2014.3.18,  
学習院大学, 東京 (招待講演)
- ⑯ K. Shiromoto,  
On critical exponents of matroids and linear codes,  
37th Australasian Conference on Combinatorial Mathematics and Combinatorial Computing, 2013. 12. 11,  
University of Western Australia, Perth, Australia.
- ⑰ K. Shiromoto,  
From codes to matroid and back,  
3rd Taiwan-Japan Conf. on Combinatorics and its Applications, 2014. 3. 21,  
National Chiayi University, Chiayi City, Taiwan (招待講演) .
- ⑱ K. Naito,  
Unpredictability of quasi-periodic dynamical systems with multiple frequencies of a p-adic extremal number and its square,  
3<sup>rd</sup> Asian Conference on Nonlinear Analysis and Optimization, 2012. 9. 4,  
Kunibiki Messe, Matue (招待講演) .
- ⑲ H. Inoue, K. Naito,  
p-adic continued fractons and a p-adic behavior of quasi-periodic dynamical systems,  
3<sup>rd</sup> Asian Conference on Nonlinear Analysis and Optimization, 2012. 9. 3,  
Kunibiki Messe, Matue.
- ⑳ T. Murakami, K. Naito,  
Spectral analysis of p-adic fractional differential operators and p-adic Schrödinger type operators,  
3rd Asian Conference on Nonlinear Analysis and Optimization, 2012. 9. 3,  
Kunibiki Messe, Matue.

[図書] (計 0 件)

[産業財産権]

○出願状況 (計 0 件)

○取得状況 (計 0 件)

[その他] ホームページ等 該当なし

## 6. 研究組織

### (1) 研究代表者

内藤 幸一郎 (NAITO, Koichiro)  
熊本大学・大学院自然科学研究科・教授  
研究者番号 : 10164104

### (2) 研究分担者

城本 啓介 (SHIROMOTO, Keisuke)  
熊本大学・大学院自然科学研究科・教授  
研究者番号 : 00343666

三沢 正史 (MISAWA, Masashi)  
熊本大学・大学院自然科学研究科・教授  
研究者番号 : 40242672

和田 健志 (WADA, Takeshi)  
島根大学・大学院総合理工学研究科・教授  
研究者番号 : 70294139

### (3) 連携研究者

小川 卓克 (OGAWA, Takayoshi)  
東北大学・大学院理学研究科・教授  
研究者番号 : 20224107