履歴書 業績 仕事の内容紹介

広島大学大学院理学研究科・教授・松本 眞

平成 22 年 3 月 17 日

勤務先
〒 739-8526 東広島市鏡山 1-3-1 広島大学大学院理学研究科　数学専攻 C707 号室
電話 082-424-7348 ファクシミリ 082-424-0710 直通 082-424-7348
電子メール：m-mat ‘‘at mark’’ math.sci.hiroshima-u.ac.jp
ホームページ: http://www.math.sci.hiroshima-u.ac.jp/~m-mat

まつもと　まこと
松本　　眞

学　歴

昭和５８年　３月３１日私立麻布高校卒業
昭和５８年　４月　１日東京大学理科１類入学
昭和６０年　４月　１日東京大学理学部情報科学科進学
昭和６２年　３月２８日同 卒業
昭和６２年　４月　１日東京大学大学院理学系研究科修士課程（情報科学専攻）入学
平成　１年　３月２９日同上修了
平成　１年　４月　１日東京大学大学院理学系研究科第一種博士課程（数学専攻）進学
平成　２年　９月３０日同 中途退学

学　位

平成　7 年　1 月 23 日 博士（理学）取得　（京都大学、論文博士）
平成 12 年　3 月 29 日 博士（工学）取得　（東京大学、論文博士）

職　歴

平成　２年１０月　１日 京都大学数理解析研究所助手
平成　７年　９月　１日 慶応義塾大学理工学部専任講師
平成１０年　４月　１日 慶応義塾大学理工学部助教授
平成１１年　４月　１日 九州大学数理学科助教授
平成１２年　４月　１日 京都大学総合人間学部基礎科学科助教授
平成１４年　４月　１日 広島大学大学院理学研究科教授

賞　罰

Institute of Combinatorics and its Applications: 1997 年度 Kirkman Medal (1998 年 3 月受賞)
日本数学会建部賢弘賞 (1998 年 10 月 1 日受賞)
慶応義塾大学 義塾賞 (1998 年 11 月 10 日受賞)
日本 IBM 科学賞 (1999 年 12 月受賞)
第 4 回船井情報科学振興賞 (2005 年 3 月 12 日受賞)
平成 18 年度科学技術分野の文部科学大臣表彰 科学技術賞（開発部門）(2006 年 4 月 18 日受賞)
平成 19 年度日本学術振興会賞 (2008 年 3 月 3 日受賞)
平成 20 年度広島大学学長賞 (2008 年 11 月 26 日受賞)

論文リスト

参考文献

[1] M. Imori, M. Matsumoto and H. Yamada “The line digraph of a regular and pancircular digraph is also regular and pancircular,” 1988・Graphs and Combinatorics 4(235–239)

[2] M. Matsumoto and N. Tokushige “The exact bound in the Erdös-Ko-Rado Theorem for cross-intersecting families,” 1989・Journal of Combinatorial Theory Ser.A 52(90–97)

[3] M. Matsumoto and N. Tokushige “A generalization of the Katona Theorem for cross t-intersecting families,” 1989・Graphs and Combinatorics 5(159–171)

[4] M. Matsumoto “Bounds for the vertex linear arboricity” 1990・Jounal of Graph Theory 14(117–126)

[5] Y. Egawa, K, Kaneko and M. Matsumoto “A mixed version of Menger’s Theorem,” 1991・Combinatorica 11(71–74)

[6] Y. Kurita and M. Matsumoto "Primitive t-nomial ($t = 3, 5$) over GF(2) whose degree is a Mersenne Exponent $\leq$ 44497," 1991 • Mathematics of Computation 56(817–821)

[7] M. Matsumoto and Y. Kurita "Twisted GFSR Generators," 1992 • ACM Transactions on Modeling and Computer Simulations 2(179–194)

[8] M. Asada, T. Oda and M. Matsumoto "Local monodromy on the fundamental groups of algebraic curves along a degenerate stable curve," 1995 • Journal of Pure and Applied Algebra (103) 235–283

[9] P. Frankl, M. Matsumoto, I. Z. Ruzsa and N. Tokushige "Minimum shadows in uniform hypergraphs and a generalization of the Takagi function," 1994 • Journal of Combinatorial Theory (A) 68(125–148)

[10] M. Matsumoto and Y. Kurita "Twisted GFSR Generators II,"

1994 • ACM Transactions on Modeling and Computer Simulation, Vol.4, No. 3 (July, 1994) (254–266)

[11] B. Chen, M. Matsumoto J. Wang, Z. Zhang, and J. Zhang, "A Short Proof of Nash-Williams' Theorem for the Arboricity of a Graph" 1994 • Graphs and Combinatorics 10(27–28)

[12] M. Matsumoto "On the Galois image in the derivation algebra of π_1 of the projective line minus three points" 1995 • Contemporary Mathematics 186(201–213)

[13] Y. Ihara and M. Matsumoto "On Galois actions on profinite completion of braid groups" 1995 • Contemporary Mathematics 186(173–200)

[14] M. Matsumoto "Galois representations on profinite braid groups on curves" 1996 • J. reine. angew. Math. 474 (169–219)

[15] F. Jaeger, M. Matsumoto, and K. Nomura "Association schemes related with type II matrices and spin models" Journal of Algebraic Combinatorics 8 (1998), 39-72.

[16] M. Matsumoto and Y. Kurita "Strong Deviations from Randomness in m-sequences based on Trinomials" 1996 • ACM Transactions on Modeling and Computer Simulation 6 (99–106)

[17] M. Matsumoto "Galois group $\mathrm{G}_{\mathbf{Q}}$, Singularity E_7, and Moduli $\mathcal{M}_3$" London Math. Soc. Lecture Note Series **243** Geometric Galois Actions 2. The Inverse Galois Problem, Moduli Spaces and Mapping class Groups. 1997 (179–218).

[18] H. Ashihara and M. Matsumoto "An Application of Finite Projective Space to Replicated Data Management" Computer Systems Science & Engineering, Vol.15 No.2 (Mar.2000) pp.87-91.

[19] M. Matsumoto and T. Nishimura "Mersenne Twister: a 623-dimensionally equidistributed uniform pseudorandom number generator" ACM Transactions on Modeling and Computer Simulation 8. (Jan. 1998) 3–30.

[20] Y. Kurita, H. Leeb and M. Matsumoto, An exercize (Exercize 14, Section 3.6, p.604) in Knuth's "The art of computer programming Vol.2, 3rd edtion" (1997).

[21] M. Matsumoto "A presentation of mapping class groups in terms of Artin groups and geometric monodromy of singularities" Mathematische Annalen 316, (2000) 401–418.

[22] M. Matsumoto "Simple cellular automata as pseudorandom m-sequence generators for built-in self-test" ACM Transactions on Modeling and Computer Simulation 8. (Jan. 1998) 31–42.

[23] H. Maehara and M. Matsumoto "Is there a circle that passes through a given number of lattice points?" European Journal of Combinatorics 19 (1998), 591-592.

[24] H. Enomoto, M. Hagita and M. Matsumoto, "A note on difference sets" Journal of Combinatorial Theory (A) 84 (1998) 133-144.

[25] 松本 眞「コイン投げで一儲けする方法–疑似乱数研究の現状」情報処理 Vol.39 No.11 (1998) 1166-1170

[26] T. Kumada, H. Leeb, Y. Kurita, and M. Matsumoto, "New primitive t-nomials ($t = 3, 5$) over $GF(2)$ whose degree is a Mersenne exponent" Mathematics of Computation Vol. 69 No. 230 (1999)) 811-814.

[27] M. Matsumoto, "A generalization of Jaeger-Nomura's Bose Mesner algebra associated to type II matrices," Ann. Inst. Fourier (Grenoble) 49 (1999), no. 3, 1027–1035.

[28] M. Matsumoto and T. Oda, "Combinatorial Dehn Twists" Far East J. Math. Sci. (FJMS) 1999, Special Volume, Part II, 137–198.

[29] M. Matsumoto and T. Nishimura, "Dynamic Creation of Pseudorandom number generator," 56–69 in: Monte Carlo and Quasi-Monte Carlo Methods 1998, Ed. H. Niederreiter and J. Spanier, Springer 2000.

[30] 松本 眞, "写像類群のアルティン群による簡明な表示" 論説、雑誌「数学」、52 巻 1 号 31–42 (2000).

[31] S. Wegenkittl and M. Matsumoto, "Getting Rid of Correlations among Pseudorandom Numbers: Discarding versus Tempering," ACM Trans. on Modeling and Computer Simulation **9**, 282–294 (1999).

[32] M. Matsumoto and A. Tamagawa "Mapping-Class-group action versus Galois action on profinite fundamental groups" American Journal of Mathematics 122 1017–1026 (2000).

[33] M. Matsumoto and T. Nishimura "A Nonempirical Test on the Weight of Pseudorandom Number Generators" 381–395 in: Monte Carlo and Quasi-Monte Carlo methods 2000, Ed. K.T. Fang, F.J.Hickernel, and H. Niederreiter, Springer-Verlag 2002.

[34] M. Matsumoto and T. Nishimura "Sum-discrepancy test on pseudorandom number generators" Mathematics and Computers in Simulation, Vol. 62 (2003), pp 431-442.

[35] R. Hain and M. Matsumoto "Weighted completion of Galois groups and Galois actions on the fundamental group of $P^1 - \{0, 1, \infty\}$" Compositio Mathematicae 139-2 (2003) 119–167.

[36] R. Hain and M. Matsumoto "Tannakian fundamental groups associated to Galois groups" MSRI Publications 41 (2003) 183–216.

[37] M. Matsumoto and S. Tagami "Practical fast algorithm for finite field arithmetics using group rings" Hiroshima Mathematical Journal 34 (2004), no. 2, 201–210

[38] R. Hain and M. Matsumoto Galois actions on fundamental groups of curves and the cycle C-C' Journal of the Inst. Math. Jussieu 4 (2005), 363-403.

[39] F. Panneton, P. L'Ecuyer and M. Matsumoto "Improved Long-Period Generators Based on Linear Reccurences Modulo 2" ACM Transactions on Mathematical Software, 32 (1, March) 2006, 1–16.

[40] Makoto Matsumoto, Mutsuo Saito, Hiroshi Haramoto, Takuji Nishimura "Pseudorandom Number Generation: Impossibility and Compromise" Journal of Universal Computer Science, Vol. 12, No. 6, pp. 672-690, 2006.

[41] 松本眞, 西村拓士, M 系列に対する重みディスクレパンシー検定, 山形大学紀要（自然科学）, Vol. 16、No. 3, 2007 年, 105–112.

M. Matsumoto and T. Nishimura, Weight discrepancy tests on M-sequences, Bulltin of Yamagata University (Natural Science), Vol. 16, No.3, 2007, 105–112.

[42] Haramoto, H., Matsumoto, M., Nishimura, T. "Computing conditional probabilities for $\mathbf{F}_2$-linear pseudorandom bit generator by splitting Mac-Williams identity", International Journal of Pure and Applied Mathematics, Vol.38 No.1, 2007.

[43] Makoto Matsumoto, Isaku Wada, Ai Kuramoto, Hyo Ashihara, "Common Defects in Initialization of Pseudorandom Number Generators," ACM Trans. on Modeling and Computer Simulation 17(4): (2007). （21 ページ）

[44] Mutsuo Saito and Makoto Matsumoto, "SIMD-oriented Fast Mersenne Twister: A 128-bit Pseudorandom Number Generator," in: Monte Carlo and Quasi-monte Carlo Methods 2006, pp. 617–632, Springer-Verlag, 2007.

[45] Makoto Matsumoto, Mutsuo Saito, Takuji Nishimura, and Mariko Hagita. "A Fast Stream Cipher with Huge State Space and Quasigroup Filter for Software," in: Carlisle M. Adams, Ali Miri, Michael J. Wiener Ed. Selected Areas of Cryptography 2007 (SAC 2007), Lecture Notes in Computer Science 4876, pp.245–262, Springer-Verlag 2007.

[46] 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).

[47] Mariko Hagita, Makoto Matsumoto, Fumio Natsu, Yuki Ohtsuka. “Error Correcting Sequence and Projective De Bruijn Graph,” Graphs and Combinatorics 24, pp.185-194 (2008)

[48] Yuki Ohtsuka, Makoto Matsumoto, and Mariko Hagita. “Projective de Bruijn Sequences,” Lecture Notes in Computer Science 5203, Sequences and Their Applications - SETA 2008, pp.167–174, 2008.

[49] Hiroshi Haramoto, Makoto Matsumoto, and Pierre L’Ecuyer. “A Fast Jump Ahead Algorithm for Linear Recurrences in a Polynomial Space,” Lecture Notes in Computer Science 5203, Sequences and Their Applications - SETA 2008, pp.290–298, 2008.

[50] Hiroshi Haramoto, Makoto Matsumoto. “A p-adic algorithm for computing the inverse of integer matrices,” Journal of Computational and Applied Mathematics 225 (2009), pp. 320-322. doi:10.1016/j.cam.2008.07.044

[51] Richard Hain, Makoto Matsumoto. “Relative Pro-ℓ Completions of Mapping Class Groups,” Journal of Algebra, vol. 321 (2009), pp. 3335-3374.

[52] 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, P. L’Ecuyer and A. Owen (Ed.), Springer-Verlag 2009. pp.589–602.

[53] Shin Harase, Makoto Matsumoto, Mutsuo Saito. “Fast lattice reduction for F_2-linear pseudorandom number generators,” To appear in Mathematics of Computation.

A. 研究活動について

現在の研究対象はおおまかに分けて以下の４つである。(a) 有限体の計算機アルゴリズムへの応用、特に疑似乱数生成 (b) 代数多様体の基本群へのガロア群の作用を通した数論 (c) グラフと組合せ論、(d) トポロジー、特に写像類群

(a) 有限体の計算機工学的応用として、乱数発生アルゴリズムの研究をしている [6][7][10][19] [22]。特に、[19]（９８年）において提唱した Mersenne Twister（MT）という乱数発生法は、従来の記録を飛躍的に塗り変える

ものの強い反響を受けた。MT は周期 $2^{19937}-1$ を持ち、623 次元空間に均等分布されることが証明されている。従来の生成法では周期は 2^{607} 程度であり 20 次元程度の均等分布性しか持たなかった。さらに、MT は計算機で高速に実現できるビット操作のみによって実現されており、標準的乱数生成ルーチンより 2 倍程度速い。

MT はまずザルツブルグ大学の研究チームにより http サイトにおいてニュースとして報じられ、ダウンロード可能な C-code として置かれた。その後、MT のホームページ

`http://www.math.keio.ac.jp/matumoto/mt.html`

を作成した。このプログラムの著作権・特許に関してすでに 300 を超える会社・研究グループから問い合わせを受けている（特許は申請せず、プログラムはフリーウェアとして配布している）。

Syracuse University のプラズマ シミュレーション研究グループは、この乱数発生法を使うことによりシミュレーション全体のスピードが１７%アップし、スーパーコンピュータの使用費を軽減したと報告してきた。

MT は国内外で高く評価され、広く普及している。JIS 規格「ランダム化の方法と手順」で最有力疑似乱数の一つとして採用が予定されている。この研究により、第 13 回 IBM 科学賞 コンピュータサイエンス部門 (賞金 300 万) を受賞した。

MT をさらに、分散処理システム上に展開することを西村氏と共同研究中である。その成果は、９８年６月 Claremont 大学で行なわれた「科学計算におけるモンテカルロ・準モンテカルロ法国際会議（第三回）」において一時間招待講演 (plenary session) で発表した。論文は Proceedings に掲載された [29].

また、ザルツブルグ大学との共同研究により、D.E.Knuth が９７年終りに刊行された The Art of Programming Vol.2 (3rd. ed) において提唱している乱数生成法の問題点を発見した（９７年ドイツ滞在中）。Knuth 氏とは彼が慶応を訪問した時に private に１時間ほど対話をする機会があった。それ以後研究上の意見交換を数回行ない、上記の問題点に関する注意が exercize の形で彼の本に採り入れられた [20]。また論文も掲載されている [31].

MT に利用された数学的手法は、フロベニウス写像による多項式の新既約性判定法、有限体係数巾級数環での非アルキメデス的付値による格子構造など、たぶんに整数論的なものであり、さらにそれを計算機アーキテクチャにフィットさせるためにプログラム技巧的手法が使われている。近年では、離散フーリエ反転を用いて疑似乱数の分布を計算する検定法である weight discrepancy test を西村氏と共同で提唱し、多くの発生法に対し安全に使える数列の長さの限界を具体的に求めた ([33])。

その他、有限体に置ける逆数演算の高速算法、離散ログなどを研究中である。

(b) ある群G（数体の絶対ガロア群およびTeichmüller Modular群を念頭においている）の$\mathbf{Q}$上定義された代数曲線Cのprofinite基本群$\pi_1(C\otimes\bar{\mathbf{Q}})$への作用について研究している。

１。Gとして有理数体の絶対ガロア群、Cとして射影直線から３点をとったものについて、Drinfeld, Anderson, Soulé, 伊原らにより研究されたweight filtrationとそれに付随するガロア群のリー環化について、Soulé元の積が消えないことを証明した[12]。（この手法は早稲田大学の角皆氏により楕円曲線の場合に一般化されている。）さらに、このリー環の次元の低い部分を計算機により具体的に求め、Deligne–伊原の予想が次元の低い部分には成立していることを確かめた。これらはワシントン大学での９３年のAMS conferenceにて発表した。代数曲線Cに代わって、組紐群を基本群とする有理数体上定義された（次元の高い）代数多様体を用い、絶対ガロア群の組紐群への作用を具体的に記述した[13]。これは伊原氏との共同研究であり、上述のAMS conferenceにて伊原氏により発表された。

この結果を一般の種数の曲線上の組紐群に拡張することに成功し、その応用として２つの結果が得られた[14]。まず、Xが代数体k上のアファイン代数曲線で基本群が非可換ならば、kの絶対ガロア群の外ガロア表現が忠実であることを示した。（Belyiの単射性定理の一般化である。Voevodskiiらによる予想であった。）次に、織田孝幸氏の曲線のモジュライ空間から生じる体の塔の不変性に関する予想を部分的に解決した。（９４年から９５年。現在、これについては、伊原、中村 博昭氏らがほぼ予想を解決している）。

組紐群を単純リー環のDynkin図形のArtin群に置き換え、そこへのガロア群への作用を射影直線引く3点の場合で記述することにも成功した。これを使って、種数３の代数曲線のモジュライスタックの基本群へのガロア作用が記述できる[17]。

また、写像類群の基本群への作用とガロア群の作用の関係が、基本群をprofinite完備化するかpro-l完備化するかで全く変わってしまうという結果を玉川安騎男氏とともに求めている[32]。

群GとしてTeichmüller Modular群をとり、Cとして種数gのn点穴つき曲線をとった場合について、群のグラフを用いて(1) その局所モノドロミーの記述とinduced filtration[8] (2) generatorとなるDehn twistsの組合せ論的記述[28] を行なった。

99年、R. Hainとの共同研究により、Deligne–伊原の予想「ガロアリー環がSoulé元で生成されること」の証明に成功し、MSRI研究所にて口頭発表を行った。2000年から2001年にかけて北大、名古屋大、東大でこの

結果について集中講義を行った。論文は Compositio Mathematicae および MSRI Publications に出版。

(c) 組合せ論関係ではグラフの彩色数、樹化数、および極値集合論に興味を持って研究している [1][2][3][4][5][9][11]。最近、スピンモデルとアソシエーションスキームの関連も研究している [15]。また、整数論的手法を用いて difference sets も研究している [24]。これら組合せ論の業績により、Institute of Combinatorics and its Applications: Kirkman Medal (1997 年) を受賞した。

(d) 曲面のトポロジーに関して、曲面の写像類群をアルティン群の商として美しく記述する事に成功した。不思議な事に、A, D, E 全ての単純有理特異点が関係式の中に現れる [21]。これに関連して、種数 3 写像類群の線形表現をヘッケ環を用いて構成する方法（矢野真道氏、京大総合人間学部・西山氏との共同研究）を求めた。

これら (a)-(d) の横断的業績に対し、1998 年日本数学会武部賢弘賞を受賞した。

口頭発表

1. 1990 年 12 月 “On the classification of locally hamming distance regular graphs.” 「代数的組合せ論」研究集会, 数理解析研究所

2. 1992 年 1 月 “Local monodromy on the fundamental groups and Dehn twists.” Computers and Geometry, 東京工業大学

3. 1992 年 2 月 “Local monodromy on the fundamental groups of algebraic curves along a degenerate stable curve.” 「代数的組合せ論」研究集会, 九州大学

4. 1993 年 1 月 “Combinatorial Dehn Twists and induced filtration.” 代数学コロキウム, 東京大学数理科学科

5. 1993 年 3 月 “Dehn Twists の組合せ論的記述 (I) 生成系.” 日本数学会, 中央大学

6. 1993 年 6 月 “TGFSR:新しい乱数発生法.” 「確率数値解析における諸問題」研究集会, 数理解析研究所

7. 1993 年 6 月 “Combinatorial Description of Dehn Twists.” 「代数的組合せ論」研究集会, 大阪教育大学

8. 1993 年 7 月 “On a graded quotient of $G_{\mathbf{Q}}$ induced from $G_{\mathbf{Q}} \to \mathrm{Out}\, \pi_1^l(\mathbf{P}^1 \setminus \{0,1,\infty\})$.” AMS summer conference “Recent Developments in the inverse Galois Problems,” Washington University, WA USA

9. 1993 年 7 月 “A Short Proof of Nash-Williams’ Theorem for the Arboricity of a Graph.” 「グラフと組合せ論」研究集会, 慶応大学理工学部

10. 1993 年 10 月 “Introduction to the filtered Galois representation theory in $\pi_1(\mathbf{P}^1 - \{0,1,\infty\})^{\mathrm{pro}-l}$.” 「モジュライ空間、ガロア表現、および L 関数」研究集会, 数理解析研究所

11. 1993 年 11 月 “Combinatorial Dehn Twists.” Algebraic Combinatorics, 九州大学理学部

12. 1994 年 3 月 “Galois Representation on Profinite Braid Groups on Curves.” 「モジュライ空間、ガロア表現、および L 関数」研究集会 II, 数理解析研究所

13. 1994 年 6 月 “Dehn Twists の組合せ論的記述とフィルトレーションへの応用” 九州大学数理学研究科談話会

14. 1994 年 7 月 “数体上の Affine 曲線の基本群が非可換なら profinite 化へのガロア群の外作用が忠実なこと” 京都大学合同数論セミナー

15. 1994 年 7 月 “Ring of Graphs” Japan Workshop on Graph Theory and Combinatorics, 慶応大学理工学部（招待講演）

16. 1994 年 7 月 “ガロア群の基本群への作用についての簡単な紹介” ３９回代数学シンポジューム、愛媛大学

17. 1994 年 9 月 “Both the mapping class group and the Galois group act on π_1, so what?” Riemann 面に関係する位相幾何学の研究集会, 北海道大学

18. 1994 年 10 月 “代数曲線上の n 点配置空間の π_1 へのガロア群の作用” 大阪大学代数幾何・複素幾何セミナー

19. 1994 年 12 月 “ガロア群と組み紐群” 京都大学数学談話会

20. 1995 年 1 月 “ガロア群の基本群への作用” 慶応大学数学談話会

21. 1995 年 3 月 “Spin models and Bose-Mesner Algebras, II” 数理研プロジェクト研究：代数的組合せ論研究集会

22. 1995 年 3 月 “曲線の組紐群へのガロア作用” 春期日本数学会 （立命館大学理工学部）

23. 1995 年 6 月 “M 系列の weight distribution の偏りについて” 「確率数値解析に於ける諸問題」研究集会（数理解析研究所）

24. 1995 年 6 月 “Galois actions on braid-type groups” Riemann 面に関係する位相幾何学の研究集会, 北海道大学

25. 1995 年 8 月 “Galois actions on braid groups and mapping class groups,” Geometry and Arithmetic of Moduli Spaces, Marseille, Luminy, France (国際研究集会)

26. 1995 年 9 月 “Spin Models, Association schemes, and Jones-Graph II,” Fifth International Colloquim on Graphs and Combinatorics, Marseille, Luminy, France (国際研究集会)

27. 1995 年 9 月 “E7 特異点変形と種数 3 の写像類群へのガロア作用” 秋期日本数学会 (東北大学)

28. 1995 年 9 月 “スピン模型と BM 代数 II” 秋期日本数学会 (東北大学)

29. 1995 年 12 月 “Jones のヘッケ環写像類群表現の genus 3 版に向けて” 写像類群に関する研究集会（東京工業大学）

30. 1996 年 2 月 “E_7 ヘッケ環と種数 3 写像類群” 数理解析研究所研究集会「ガロア群と写像類群の基本群への作用」

31. 1996 年 6 月 “Monstrously Long Period Pseudorandom Number Generator” Workshop on pseudorandom number generation, Montreal, Université de Montreal, Canada (国際研究集会)

32. 1996 年 10 月 “E_7 ヘッケ環と種数 3 の代数曲線の写像類群” 京都大学総合人間学部数学教室談話会

33. 1996 年 10 月 “曲面のトポロジーと数論的基本群（サーベイ）” 「リーマン面に関連する位相幾何学」, 北大数学教室研究集会

34. 1997 年 4 月 “Nonexistence and Relative Existence of Difference Sets on Some Abelian Groups” Institute IMAG, Laboratoire Leibniz, Grenoble France.

35. 1997 年 5 月 “Mersenne Twister: an implementation of a monstrous random number generator” Department of Mathematics, University of Salzburg, Austria.

36. 1997 年 6 月 “Mapping class group as quotient of Artin groups” Department of Mathematics, University of Bonn, Germany

37. 1997年6月 “Topological methods in studying Galois actions” Oberwolfach Conference on Galois groups and fundamental groups, Germany.

38. 1997年6月 “Comparison between Galois action and Mapping class group action” University of Lille, Lille France.

39. 1997 年 7 月 “Artin Groups and Presentation of Teichmüller modular groups” Department of Mathematics, University of Bielefeld, Germany.

40. 1997 年 7 月 “Tangential Morphisms”, University of Essen, Germany.

41. 1997年7月 “Comparison between Galois action and Mapping Class group action” University of Köln, Germany.

42. 1997 年 8 月 “A topological method in studying actions of absolute Galois groups on fundamental groups: Part I and II” (two days) Max-Planck-Institute for Mathematics, Bonn, Germany endenumerate

43. 1997 年 12 月 “写像類群とアルティン群” 九州大学組合せ論セミナー

44. 1998 年 1 月 “Artin Groups and Mapping Class groups” Number Theory Seminar at Max-Planck-Institute for Mathematics, Bonn, Germany.

45. 1998 年 1 月 “Mersenne Twister: 623 次元均等分布疑似乱数発生法” 「確率論と計算数学」研究集会、九州大学

46. 1998 年 2 月 “アルティン群と写像類群へのガロア作用” 東京都立大学 Dessin D’Enfants セミナー

47. 1998 年 2 月 “アルティン群と写像類群（ヘッケ環表現に向けて）” 京都大学総合人間学部数学教室談話会

48. 1998 年 3 月 “Fundamental group of algebraic variety over $\mathbf{Q}$” フランス・ニース大学数学科談話会

49. 1998 年 3 月 “Galois action on braid groups on curves” フランス・ニース大学 Seminaire de Algebra et Topologie

50. 1998 年 3 月 “623 次元均等分布疑似乱数発生法” 日本数学会応用数学分科会 特別講演 （名城大）

51. 1998 年 4 月 “ガロア群と写像類群の基本群への作用の比較” （数理研玉川氏との共同研究）東北大理学部数学教室代数セミナー

52. 1998 年 4 月 “写像類群のアルティン群による表示” 東北大理学部数学教室代数幾何セミナー

53. 1998 年 5 月 “Presentation of Mapping Class Groups In Terms Of Artin Groups” 研究集会「写像類群を巡る最近の進展」東京大学

54. 1998 年 6 月 “Dynamic Creation of Random Number Generators” 第 3 回モンテカルロ法国際会議、招待講演 Claremont, California

55. 1998 年 7 月 “写像類群のアルティン群による簡明な表示” トポロジーシンポジウム、山口大学

56. 1998 年 9 月 “A generalization of Jaeger-Nomura’s algebra associated with type II matrices” Francois Jaeger 追悼記念研究集会、Grenoble, France.

57. 1998 年 9 月 “写像類群のアルティン群による表示 I, II” Riemann 面に関連する位相幾何学、北大

58. 1998 年 10 月 “Deformation of simple singularities and presentation of mapping class groups” 東大トポロジーセミナー、東大

59. 1998 年 12 月「モンテカルロ用疑似乱数の動向」日本金融・証券計量・工学学会冬期大会、慶応大

60. 1999 年 1 月「メルセンヌ・ツイスター疑似乱数発生法」慶応大物理理論研セミナー、慶応大

61. 1999 年 2 月 24 日”Presentation of mapping class groups in terms of Artin groups” Topology and Geometry Seminar, Duke University

62. 1999 年 3 月 2 日”Absolute Galois groups and Mapping Class groups acting on the profinite fundamental groups” Topology and Geometry Seminar, Duke University

63. 1999 年 3 月 3 日”Pseudorandom number generator with period $2^{19937} - 1$” Topology and Geometry Seminar, Duke University

64. 1999 年 3 月 12 日 “An Irreducibility Test of a Polynomial over a two Element Field” Thirtieth Southeastern International Conference on Combinatorics, Graph Theory, and Computing, Florida Atlantic University.

65. 1999 年 3 月 23 日 “Dynamic Creation of Distributed Random Number Generators” Ninth SIAM Conference on Parallel Processing for Scientific Computing, San Antonio, USA.

66. 1999 年 3 月 28 日「リンゴが落ちたって万有引力は発見できないさ」（今の学問、社会のニーズに惑わされてない？）数学会市民講演会、学習院大学

67. 1999 年 4 月 2 日「メルセンヌツイスター疑似乱数発生法」理財工学研究センター設立記念シンポジウム、東工大

68. 1999 年 6 月 9 日「疑似乱数における $\mathbf{F}_2[t] \subset \mathbf{F}_2((t^{-1}))$ 格子構造の利用」九州大学数理学研究科 談話会

69. 1999 年 7 月 “Arithmetic fundamental groups and moduli of curves” 連続講義, Summer school on algebraic geometry, The Abdus Salam International Centre for Theoretical Physic, Trieste, Italy.

70. 1999 年 8 月 “Presentation of Mapping Class Groups in terms of Artin Groups,” Summer school on algebraic geometry, The Abdus Salam International Centre for Theoretical Physic, Trieste, Italy.

71. 1999 年 10 月 14 日 “Weighted Completion of the Galois Group and the Deligne-Ihara’s Conjecture” with R. Hain, Galois groups and funamental groups conference, MSRI, Berkeley, USA.

72. 1999 年 12 月 24 日「ガロア群のマルセフ完備化と Deligne-伊原の予想」代数学談話会、東京大学数理科学研究科

73. 2000 年 1 月 27 日 “Weighted Completion of the Galois Group and the Deligne-Ihara’s Conjecture” with R. Hain, 代数的整数論とその応用、京大数理解析研究所

74. 2000 年 5 月 12 日「辺の長さの与えられた単体は、何次元空間の有理点に埋め込めるか」京都大学数論合同セミナー、京都大学理学部数学科

75. 2000 年 6 月 26 日–30 日「ガロア群と基本群」集中講義、北海道大学理学系研究科数学専攻

76. 2000 年 8 月 8 日「ガロア群の代数群による完備化と基本群への表現」代数学シンポジウム、九州大学六本松キャンパス

77. 2000 年 9 月 12 日「ガロア群と写像類群の相対マルセフ完備化と Deligne の予想」研究集会「リーマン面に関連する幾何学」、大阪市立大学

78. 2000 年 10 月 24 日「ガロア群のマルセフ完備化と Deligne-伊原の予想」城崎代数幾何シンポジウム、城崎

79. 2000 年 11 月 28 日 “Deviation of weight in m-sequences” Fourth international conference on Monte Carlo and Quasi Monte Carlo method, Hongkong Baptist University.

80. 2000 年 3 月 8 日「コイン投げで儲ける方法：疑似乱数の偏差と符号理論を使った検定」応用数理セミナー、京大数理解析研究所

81. 2001 年 5 月 21 日 “Weighted completion of arithmetic mapping class groups and $C - C^-$” Workshop on Hodge theory, Galois theory, moduli and arithmetic geometry, 京大総合人間学部

82. 2001 年 9 月 “Weighted completion of Galois groups and mapping class groups” Arithmetic geometry and arithmetic fundamental groups, EURESCO Conference, Italy.

83. 2001 年 9 月 “Sum-discrepancy test on pseudorandom number generators” MCM2001 (Monte Carlo Method 2001), Salzburg Univ.

84. 2002 年 6 月 “How to make money by coin tossing” Workshop for random number generation and highly uniform point set, Universite de Montreal. (招待講演)

85. 2002 年 6 月 “How to make money by coin tossing” 九州大学大学院数理学研究院談話会

86. 2002 年 7 月「代数群によるガロア群や写像類群の近似」九州大学大学院数理学研究院代数学セミナー

87. 2003 年 5 月「代数と乱数」名古屋大学談話会

88. 2003 年 11 月 “Practical Fast Algorithm for Finite Field Arithmetics” 国際シンポジウム EACAC2, 九州大学

89. 2003 年 12 月「コイン投げで一儲けする方法」大阪大学理学部数学科談話会

90. 2004年8月基本群への外Galois表現とそのLie環化整数論サマースクール「基本群とGalois表現」(福山勤労総合福祉センター「ローズイン備後ハイツ」)

91. 2004年1月「コイン投げで一儲けする方法」京都大学総合人間学部基礎科学科談話会

92. 2004年9月「擬似乱数:「精密なデタラメさ」のジレンマ」2004年電子情報通信学会, 徳島大学

93. 2005年3月“ Galois representations in fundamental groups and their Lie algebras ”, Arizona Winter School 2005, University of New Mexico, 招待講演.

94. 2005年5月“ Common Defects in Initialization of Pseudorandom Number Generators ”, MCM2005, Fifth IMACS Seminar on Monte Carlo Methods, Florida State University.

95. 2005年5月 “Mersenne Twister and Fubuki stream/block cipher,” SKEW - Symmetric Key Encryption Workshop, Scandinavian Congress Center, Aarhus, Denmark.

96. 2005年7月”The action of the Galois group on the Lie algebra of the fundamental groups”, Asian Mathematical Conference 2005, National University of Singapore, 招待講演.

97. 2005年11月“ Generating Randomness by deterministic computations: impossibility, compromise, and assurance ”, 日独先端科学シンポジウム, 湘南国際村センター, 招待講演.

98. 2005年11月“ ストリーム暗号CryptMT ”, AC2005, 首都大学東京.

99. 2006年1月12日 “擬似乱数:危険な発生法とMersenne Twister” ＩＳＭオープンフォーラム、統計数理研究所. 招待講演。

100. 2006年1月13日 “デタラメさを精密につくる:「１＋１＝０」の数学の乱数生成への応用,” 筑波大学第一学群自然学類文化講演会. 招待講演。

101. 2006年1月“ Analysis of Cryptographic Mersenne Twister ”, SCIS2006, 電子通信学会、広島プリンスホテル.

102. 2006年2月“ CryptMT: effect of huge prime period and multiplicative filter, and a tweak on faster initialization. ”, SASC2006 - Stream Ciphers Revisited, College De Valk, Leuven, Belgium .

103. 2006 年 8 月 3 日 “ Random number generation: yet another application of algebra,“ 2006 Workshop on Cryptography and Related Mathamatics, Chuo Univ. 東京、国際研究集会、招待講演

104. 2006 年 8 月 14 日 “Pulmonary Mersenne Twister pseudorandom number generator,” with Hiroshi Haramoto, Mutsuo Saito, Takuji Nishimura, and Francois Panneton. MCQMC2006, University of Ulm, Germany 国際研究集会

105. 2006 年 10 月 24 日 “Malcev completions of arithmetic mapping class groups” with R. Hain, Arithmetic Galois Theory and Related Moduli Spaces, 京都大学数理解析研究所, 国際研究集会

106. 2006 年 11 月 25 日 “Malcev type completion of arithmetic mapping class groups,” with R. Hain, P-adic method and its applications in arithmetic geometry, 広島大学、国際研究集会

107. 2007 年 1 月 5 日 “Evaluation of Pseudorandom Number Generators for Monte Carlo Simulation” ISM Workshop. 統計数理研究所、国際研究集会、招待講演

108. 2007 年 2 月 1 日 “CryptMT Ver. 3: Speed-up by considering recent parallelism in modern CPUs” SASC2007, Ruhr University, Germany, 国際研究集会

109. 2007 年 3 月 7 日 “ Random number generation: yet another application of algebra,“ MRA2007, 広島大学、国際研究集会

110. 2007 年 3 月 27 日 “間違いだらけの疑似乱数選び” 熊本大学工学部講演会

111. 2007 年 4 月 5 日 “ デタラメさを精密につくる：メルセンヌツイスター擬似乱数発生法,” 産業技術総合研究所、千里中央、招待講演。

112. 2007 年 4 月 6 日 “ デタラメさを精密につくる：メルセンヌツイスター擬似乱数発生法,” OR 学会中国四国支部講演会, 広島大学東千田キャンパス、招待講演。

113. 2007 年 8 月 17 日 “A fast stream cipher with huge state space and quasigroup filter for software,” The 14th Annual Workshop on Selected Areas in Cryptography (SAC2007), University of Ottawa.

114. 2007年9月15日 “Relative pro-l completion of fundamental groups,” Asian Conference on Arithmetic Geometry 2007, Korea Institute of Adavanced Study. 招待講演。

115. 2008年1月5日 “メルセンヌツイスター：SIMD高速タイプ(SFMT)と暗号耐性化(CryptMT)” 平成１９年度統計数理研究所 乱数重点型共同研究第2回研究会乱数の応用指向特性評価とその周辺（応用)、統計数理研究所,　招待講演。

116. 2008年7月6－11日 Random Number Generation and Evaluation I, II Session organizer. MCQMC2008, University of Montreal.

117. 2008年7月9日 “Generating uniform real random numbers in IEEE 754 specification via affine transition” (presented by Mutsuo Saito) MCQMC2008, University of Montreal.

118. 2008年12月13日 “擬似乱数検定における、サンプルサイズ調整の自動化” 平成２０年度統計数理研究所 乱数重点型共同研究第2回研究会統計数理研究所。

119. ２００９年8月２８日 Differences between Galois representations in automorphism and outer-automorphism groups of the fundamental group of curves “Anabelian Geometry” workshop 8/24–28 Newton Institute, Cambridge (Invited Speaker).

120. 2009/9/16 “Study of Galois representations via Teichmüller modular groups.”

    The international symposium Geometry and Analysis of Automorphic Forms of Several Variables, 14–17, September 2009 at Tokyo in honor of Professor Takayuki Oda on the occasion of his 60th birthday (Invited Speaker)

121. 2009/10/20 “Relations among Dehn twists given by deformation of simple singularities” 広島大学トポロジー幾何セミナー、依頼講演

1　その他の教育活動

1. 1992年8月：数理解析研究所市民公開講座「グラフと組合せ論」
2. 1994年6月：九州大学数理学研究科集中講義 「Combinatorial Dehn Twists」

3. 1998 年 7 月：琉球大学教育学部集中講義「有限体とその応用」
4. 2000 年 6 月：北海道大学理学系研究科数学専攻集中講義「ガロア群と基本群」
5. 2000 年 9 月：名古屋大学理学系研究科数学専攻集中講義「ガロア群の重みつきマルセフ完備化とモチーフ」
6. 2001 年 7 月：東京大学数理科学研究科集中講義「ガロア群の重みつきマルセフ完備化」
7. 2001 年：金沢大学理学部数学科集中講義「有限体の工学的応用」
8. 2003 年 12 月：大阪大学理学部数学科集中講義「有限体の工学的応用」
9. 2004 年 1 月：京都大学総合人間学部基礎科学科集中講義「有限体と擬似乱数」
10. 2004 年 7 月：山形大学理学部集中講義「有限代数と擬似乱数」
11. 2004 年 11 月：東京工業大学理学部集中講義「有限代数と擬似乱数」

2　外部評価資料

松本 眞 (教授、京都大学博士（理学)、東京大学博士（工学）) 広島大学大学院　理学研究科　数学専攻

2.1　研究業績

以下の 4 つの分野において研究を行なっている。(a) 有限体の計算機アルゴリズムへの応用、特に疑似乱数生成 (b) 代数多様体の基本群へのガロア群の作用を通した数論 (c) グラフと組合せ論、(d) トポロジー、特に写像類群

発表論文は別セクション（上の方）を参照

2.2　外部資金受け入れ状況

- 平成 8 年度 科研費 奨励 A 研究課題「曲線のモジュライ空間の幾何を介した外ガロア表現の研究」

  8 年度 100 万円

  代表者 松本 眞

- 平成 9–10 年度科研費 奨励 A

  研究課題「写像類群のヘッケ環表現とガロア作用」

  9 年度 120 万円 10 年度 120 万円

  代表者 松本 眞

- 平成 11–12 年度科研費 奨励 A

  研究課題「単純特異点の変形空間と曲線のモジュライ」

  11 年度 110 万円 12 年度 110 万円

  代表者 松本 眞

- 平成 13–15 年度科研費 基盤 B

  研究課題「モジュライ空間の幾何とガロア作用」

  代表者 松本 眞

  13 年度 230 万円

  14 年度 250 万円

  15 年度 250 万円

- 平成 14–16 年度科研費 萌芽課題番号 14654021 研究課題「並列分散モンテカルロ法と擬似乱数」

  代表者 松本 眞

  14 年度 100 万円

  15 年度 130 万円

  16 年度 60 万円

- 平成 16–19 年度科研費 基盤 A

  研究課題「古典的数論幾何学の枠組みを超えて— ゼータ・数論的トポロジー・圏論的数論幾何」課題番号 16204002 代表者 松本 眞 直接経費額 16 年 650 万円、17 年 650 万円、18 年 570 万円、19 年 570 万円

  (最終年度：前年度申請採択により打ち切り)

- 平成 18–19 年度先端研究拠点事業－拠点形成型－「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」採用番号 18005 研究代表者 松本 眞

  Ｈ１８年８８０万円Ｈ１９年１３０３万円

- 平成 18–20 年度科研費　萌芽研究「高性能線形擬似乱数の開発と非線形化、暗号耐性化の研究」課題番号　18654021 研究代表者　松本　眞Ｈ１８年１００万、Ｈ１９年９０万、Ｈ２０年８０万
- 平成 19–22 年度科研費　基盤A研究課題名「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」課題番号 19204002 研究代表者　広島大学大学院理学研究科　松本　眞直接経費額　H19 7,500,000　H20 6,200,000　H21 6,300,000　H22 6,300,000
- 平成 20–22 年度先端研究拠点事業－国際戦略型－「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」採用番号　18005 研究代表者　松本　眞

  Ｈ２０年１６５９．９万円Ｈ２１年２２００万円Ｈ２２年未定
- 平成 21–23 年度科研費　資金制度・研究費名 挑戦的萌芽研究期間　H21–H23 配分機関名 広島大学研究課題名「新世代高機能擬似乱数発生法の開発」研究代表者氏名　松本　眞

  課題番号：21654017

  内定額：21 年：1,000,000 22 年：1,000,000 23 年：1,000,000

その他の外部資金

- 株式会社大広「テレビ通販枠に関する要求付き公平割り付け問題に関するアルゴリズムの開発」165 万円

  H19/7/1–H20 (共同研究)

2.3　外国人学者受け入れ

- 2001 年 5 月 (3 週間)　Duke 大学数学科 R.Hain 教授
- 2002 年 12 月 (2 週間)　Duke 大学数学科 R.Hain 教授
- 2003 年 10-12 月 (2.5 月)　Arizona 大学数学科 Kim Minhyong 助教授
- 2005 年 1 月 (7 日間)　Francois Panneton 博士
- 2005 年 2 月 (9 日間)　パリ高等師範大学数学科 Yves.Andre 教授

2.4　海外との共同研究

1998 年 3 月（1 カ月)、2000 年 7 月 18 日–8 月 3 日、2004 年 6 月 5 日–17 日、アメリカ Duke 大学に出張して 数学教室 R.Hain 教授と共同研究。

98 年 3 月は慶応義塾大学の資金、00 年 7 月ー 8 月および 04 年 6 月は科研費。受け入れ教官は R.Hain 教授。

2.5　学外活動

通産省 JIS 規格「JISZ903 乱数発生及びランダム化の手順」改正原案作成委員会委員（1998 年 4 月–1999 年 3 月）日本数学会代数学分科会運営委員（2003 年 4 月–現在）日本数学会評議員（2003 年 4 月ー 2004 年 3 月）日本数学会「数学」編集委員（2002 年 7 月ー 2006 年 6 月）日本学術会議連携会員 (2006 年 8 月-2008 年 9 月)