Alina Ostafe

University of New South Wales
School of Mathematics and Statistics
Sydney NSW 2052
Australia

Office: Red Centre, 4078
Tel.: +61 (02) 93853976
Email: alina.ostafe@unsw.edu.au
Website: http://web.maths.unsw.edu.au/~alinaostafe/

Personal information

Date of birth: January 18, 1982
Citizenship: Australian, Romanian

Education

2010	*PhD*, Institute of Mathematics, University of Zürich, Switzerland PhD thesis: "*Polynomial Dynamics and Pseudorandomness*" Supervisors: Prof. Joachim Rosenthal, Prof. Markus Brodmann
2007	*MSc*, Faculty of Mathematics, University of Bucharest, Romania Diploma thesis: "Generalized Alexander Duality and Applications"
2005	*Diploma in advanced undergraduate studies (Mathematics)*, Scoala Normala Superioara Bucharest, Romania
2005	*BSc*, Mathematics and Informatics Ovidius University, Constanta, Romania

Current positions

Since 2018	*Senior Lecturer*, School of Mathematics and Statistics, The University of New South Wales (UNSW), Sydney, Australia

Previous positions

2016–2018	*Lecturer*, School of Mathematics and Statistics, UNSW, Sydney, Australia
2013–2016	*Vice-Chancellor's Postdoctoral Fellow*, School of Mathematics and Statistics, UNSW, Sydney, Australia
2010–2013	*Postdoc*, Department of Computing, Macquarie University, Sydney, Australia (funded by the Swiss National Science Foundation Grants 133399 and 139679 and the Australian Research Council)
2007–2010	*Research/Teaching Assistant*, Institute of Mathematics, University of Zürich, Switzerland
2005–2007	*Research Assistant*, Institute of Mathematics "Simion Stoilow" of the Romanian Academy, Bucharest, Romania

Research Interests

Number Theory (Diophantine problems; Polynomials and rational functions over local and global fields; Finite fields; Matrices)
Arithmetic dynamical systems

Fellowships and Grants

2020–2022	Australian Research Council Discovery Project (435,000 AUD) (with I. Shparlinski)
2019	NSW Department of Industry Conference funding (4,000 AUD) (with J. Roberts, I. Shparlinski and L. Zhao)
2018–2020	Australian Research Council Discovery Project (401,706 AUD) (with J. Roberts and I. Shparlinski)
2017	UNSW Science Faculty Research Grant (6,500 AUD)
2017	UNSW Start-up Grant (10,000 AUD)
2016	UNSW Science Faculty Research Grant (8,364 AUD)
2015	UNSW Science Faculty Research Grant (7,400 AUD)
2014	Workshop AMSI/AustMS–AMSI/ANZIAM funding (20,000 AUD) (with B. McKay, J. Roberts and I. Shparlinski)
2013–2016	UNSW Vice-Chancellor's Postdoctoral Fellowship (310,000 AUD)
2012–2013	Swiss National Science Foundation Grant for Advanced Researchers (76,500 CHF)
2010–2012	Swiss National Science Foundation Grant for Prospective Researchers (67,300 CHF)

Organisation of research meetings

2022	Specialisation and Effectiveness in Number Theory *Banff International Research Station* Alberta, Canada (with C. Stewart, R. Tichy, J. Wang)
2019	Number Theory Down Under 7, *UNSW Sydney*, Australia (with J. Roberts, I. Shparlinski, L. Zhao)
2016	Dynamics and Graphs over Finite Fields: Algebraic, Number Theoretic and Algorithmic Aspects, *Centre International de Rencontres Mathématiques*, Luminy, France (with M.-C. Chang, J. von zur Gathen and F. Pappalardi)
2015	Workshop on Algebraic, Number Theoretic and Graph Theoretic Aspects of Dynamical Systems, *UNSW Sydney*, Australia (with B. McKay, J. Roberts and I. Shparlinski)
2014	Polynomials over Finite Fields: Functional and Algebraic Properties *Centre de Recerca Matematica*, Barcelona, Spain (with J. von zur Gathen, J. Gutierrez, D. Panario and A. Topuzoglu)
2013	Finite fields and their applications *Johann Radon Inst. for Computational and Applied Math.* (RICAM), Linz, Austria (with H. Niederreiter, D. Panario and I. Shparlinski)
2013	The Art of Iterating Rational Functions over Finite Fields *Banff International Research Station*, Alberta, Canada (with N. Boston, I. Shparlinski, M. Zieve)

Organisation of online international events

Since 2020	Number Theory Web Seminar (twice a week in 2020; every Thursday from 2021) (with M. Bennett and P. Habegger) `https://www.ntwebseminar.org/home`
2020	Number Theory Online Conference 2020 (with F. Breuer, M. Coons and T. Morrill) `https://carma.newcastle.edu.au/meetings/ntoc2020/`

Research in Pairs programs

2015	*Mittag-Leffler Institute*, Sweden (2 weeks) (with O. Ahmadi, D. Gomez-Perez and M. Sha)
2015	*Mathematisches Forschungsinstitut Oberwolfach*, Germany (2 weeks) (with O. Ahmadi, D. Gomez-Perez and M. Sha)

2013 *Centre International de Rencontres Mathematiques*, Luminy, France (2 weeks)
(with D. Gomez-Perez)
2013 *Mathematisches Forschungsinstitut Oberwolfach*, Germany (2 weeks)
(with D. Gomez-Perez)

Member of conference scientific committees

2021 AustMS 2021, University of Newcastle, Australia
2021 Number Theoretical Methods in Cryptology, Poznan
2020 Diophantine Problems: Determinism, Randomness, Applications, CIRM, France
2020 Algorithmic Number Theory Symposium, ANTS 2020, University of Auckland, New Zealand
2019 Number Theoretical Methods in Cryptology, Paris
2018 Algorithmic Number Theory Symposium, ANTS 2018, University of Wisconsin, USA
2014 Sequences and their Applications, SETA 2014, University of Melbourne, Australia
2013 The 11th International Conference on Finite Fields and their Applications, Fq11
Otto-von-Guericke-University Magdeburg, Germany

Other mathematical memberships

Since 2018 Australian Mathematical Society
Since 2018 Number Theory Down Under
2018 American Mathematical Society (awarded)

Institutional responsibilities

Since 2021 *Director of Postgraduate Studies - Future Students*, UNSW, Sydney
Since 2021 *Member of the Research Committee*, UNSW, Sydney
Since 2021 *Member of the Academic Committee*, UNSW, Sydney
Since 2021 *Secretary of the Australian Mathematical Society Interest Group*
Number Theory Down Under
2019–2021 *President of the Australian Mathematical Society Interest Group*
Number Theory Down Under
Since 2017 *Member of the Science Faculty Board*, UNSW, Sydney
Since 2017 *Postgraduate Review Committee Member*, UNSW, Sydney
Since 2015 *Organiser of Number Theory Seminar*, UNSW, Sydney
(co-organiser with David Harvey)
2018, 2017, 2014 *Lecturer/Sen. Lecturer/Postdoc hiring committees member*, UNSW, Sydney

Teaching activities

UNSW, Sydney, Australia:

2021
- *Lecturer*: MATH2099 (Linear Algebra)
- *Lecturer and course authority*: MATH5645 (Algebraic Number Theory)

2020
- *Lecturer*: MATH1141 (Algebra)
- *Lecturer and course authority*: MATH5725 (Galois Theory)

2019
- *Lecturer*: MATH1141 (Algebra)
- *Lecturer and course authority*: MATH5645 (Algebraic Number Theory)
- *Tutor*: MATH1141 (Algebra), MATH1151 (Algebra)

2018
- *Lecturer*: MATH1141 (Algebra), MATH1131 (Calculus)
- *Lecturer and course authority*: MATH5725 (Galois Theory)
- *Tutor*: MATH1141 (Algebra), MATH1231/1241 (Algebra)

2017
- *Lecturer*: MATH1141 (Algebra)
- *Lecturer and course authority*: MATH5645 (Algebraic Number Theory)
- *Tutor*: MATH1141 (Algebra), MATH1231/1241 (Algebra)

2015 *Lecturer (on voluntary basis)*: MATH5645 (Finite Fields and Applications)

University of Zürich, Switzerland:

2010	*Design and conducting* a student seminar on Pseudorandom Sequences
2009	*Tutor*: Linear Algebra II, Elliptic Curves
2008	*Tutor*: Linear Algebra I

Student supervision

2021	Conrad Martin, *Powers in orbits of rational dynamical systems* (Honours)
2019	Alexander Patterson, *Polynomial dynamics over number fields: irreducibility of iterates and powers in orbits* (Honours)
2018	Marley Young, *The arithmetic of semigroup dynamical systems over the cyclotomic closure of a number field* (Honours)
2017	Marley Young, *On the multiplicative independence of iterates of rational functions* (summer project, co-supervisor)
2016	Johann Blanco, *Dynamics of monomials and Dickson polynomials over finite fields* (Honours)

Postdoc supervision

2019 - 2021	Jorge Mello (co-supervised with J. Roberts and I. Shparlinski)

Organiser of outreach and student activities

Since 2018	*Annual Information Session 'Becoming a PhD student: What does it take?'*, UNSW, Sydney
2019	*Girls Do The Maths & Public Lecture by Prof. Kate Smith-Miles*, UNSW, Sydney (co-organiser with A. Liebenau and D. Salopek)
2018	*Advanced Mathematics Day*, UNSW, Sydney (co-organiser with S. Waters)
2018	*Girls Do The Maths & Public Lecture by Prof. Cheryl Praeger*, UNSW, Sydney (co-organiser with D. Combe and D. Salopek)

Other outreach and student activities

2016	*Advanced Mathematics Day*, UNSW, Sydney (invited speaker)

Reviewer for funding agencies

Since 2018	Australian Research Council (ARC)
2015	National Security Agency (NSA), USA
2013	Austrian Science Fund (FWF)

Reviewer for journals and conference proceedings

- *Journals (since 2010):* Algebra and Number Theory; Finite Fields and Their Applications; Bulletin of the Australian Mathematical Society; Journal of Number Theory; International Journal of Number Theory; Journal of Algebra and its Applications; New York Journal of Mathematics; Quaestiones Mathematicae; Linear Algebra and its Applications; Discrete Mathematics; Designs, Codes and Cryptography; SIAM Journal on Discrete Mathematics; SIAM Journal on Computing; Journal of the Australian Mathematical Society; IEEE Transactions on Computers;
- *Conference proceedings (since 2009):* ANTS XIV; The 11th International Conference on Finite Fields and their Applications; Computer Algebra in Scientific Computing; International Workshop on Public Key Cryptography, PKC′10; The 9th International Conference on Finite Fields and Applications
- *Handbooks (2011):* Handbook of Finite Fields, CRC Press, Eds. G. Mullen and D. Panario
- *Mathematical Reviews (since 2010)*

Research visits

2020, 2017, 2016, 2015, 2014	Max Planck Institute for Mathematics, Bonn (3 months, 2014; 2 weeks, 2015; 2 weeks, 2016; 1 week 2017; 11 months, 2020)
2020, 2019, 2010	RICAM, Linz, Austria (2 weeks, 2010; 2 × 4 days, 2019; 1 week, 2020)
2019	University of Debrecen, Hungary (4 days)
2018, 2014, 2012, 2011	University of Cantabria, Santander, Spain (2 weeks, 2011; 1 week, 2012; 1 week, 2014; 2 weeks, 2018)
2017	Alfréd Rényi Institute of Mathematics, Budapest, Hungary (4 days)
2017	Australian National University, Canberra, Australia (2 days)
2017	Fields Institute, Toronto, Canada (2 weeks) (attending the Thematic Program on Unlikely Intersections, Heights, and Efficient Congruencing)
2016	Scuola Normale Superiore Pisa, Italy (1 week)
2016	Magdeburg University, Germany (1 week)
2015	Technical University (TU) Graz, Austria (1 week)
2013	Bielefeld University, Germany (3 days)
2013	Univeristy of Neuchatel, Switzerland (2 weeks)
2012	ICERM, Brown University, USA (2 weeks)
2012, 2011	Sabanci University, Istanbul, Turkey (2 weeks, 2011; 1 week, 2012)
2011	Phillips Research, Eindhoven, Netherlands (1 week)
2011	The Erwin Schrödinger Intern. Institute for Mathematical Physics (ESI) Vienna, Austria (2 weeks)
2011	NTU, Singapore (3 days)
2011	Universidad Autonoma de Madrid, Spain (1 week)

Research Talks[1]

December 2022	Pacific Rim Mathematical Association Congress – Arithmetic Geometry Session
October 2021	Number Theory Meeting – Torino, Italy (online)
September 2021	Number Theory Down Under 9, University of Sydney, Australia (online)
February 2021	7th International Conference on Uniform Distribution Theory, RICAM, Linz, Austria (online)
January 2021	Number Theory Seminar, Max Planck Institute for Mathematics, Bonn, Germany (online)
December 2020	Tel Aviv Number Theory Seminar (online)
November 2020	Diophantine Problems, Determinism and Randomness, CIRM, Luminy (online)
March 2020	Algebra, Geometry and Physics Seminar, Max Planck Institute for Mathematics, Bonn, Germany
February 2020	Number Theory Seminar, University of Cambridge, UK
February 2020	Oberseminar, Max Planck Institute for Mathematics, Bonn, Germany
January 2020	Mathematics Colloquium, TU Graz, Austria
November 2019	Algebra Seminar, University of Sydney, Australia
September 2019	Intercity Number Theory Seminar, Radboud University Nijmegen, The Netherlands
July 2019	Number Theory Colloquium, TU Graz, Austria
July 2019	Colloquium Talk, RICAM, Linz, Austria
July 2019	Number Theory Seminar, Alfréd Rényi Institute of Mathematics, Budapest, Hungary
June 2019	Dynamics and Number Theory, University of Sydney, Australia
May 2019	Arithmetic of Function Fields and Diophantine Geometry, Taipei, Taiwan
March 2019	Arithmetic Dynamics Session, AMS Joint Sectional Meeting, University of Hawaii, USA
January 2019	Research Seminar, RICAM, Linz, Austria
January 2019	Number Theory Seminar, IST, Austria
September 2018	Number Theory Down Under, UNSW Canberra, Australia
March 2018	Number Theory Seminar, UNSW, Sydney, Australia
January 2018	Arithmetic Dynamics Session, AMS Joint Mathematics Meetings, San Diego, USA

[1] All talks which are not indicated as seminar/colloquium talks were given at conferences/workshops that I attended.

December 2017	Number Theory Seminar, Max Planck Institute for Mathematics, Bonn, Germany
July 2017	Number Theory Seminar, Alfréd Rényi Institute of Mathematics, Budapest, Hungary
June 2017	Algebra Seminar, University of Sydney, Australia
January 2017	Colloquium, Australian National University, Canberra, Australia
December 2016	Number Theory Seminar, Max Planck Institute for Mathematics, Bonn, Germany
December 2016	Seminar talk, Magdeburg University, Germany
December 2016	Seminar talk, Scuola Normale Superiore Pisa, Italy
September 2016	Number Theory Down Under, Newcastle, Australia
September 2016	Conference on Elementary and Analytic Number Theory, Strobl, Austria
August 2016	Workshop on Arithmetic Dynamics, University of Basel, Switzerland
August 2016	Cryptography and Coding Theory Seminar, University of Neuchatel, Switzerland
April 2016	Number Theory Seminar, Max Planck Institute for Mathematics, Bonn, Germany
December 2015	Seminar Talk, University of Salzburg, Austria
December 2015	Interview talk, Hausdorff Center for Mathematics, Bonn, Germany
November 2015	Number Theory Seminar & Colloquium (2 talks), TU Graz, Austria
September 2015	Cryptography and Coding Theory Seminar, University of Neuchatel, Switzerland
June 2015	Elementary, Analytic, and Algorithmic Number Theory: Research inspired by the Mathematics of Carl Pomerance, University of Georgia, Athens, USA
May 2015	The First Mini Symposium of the Roman Number Theory Association, Università Europea di Roma, Rome, Italy
April 2015	Number Theory Seminar, Max Planck Institute for Mathematics, Bonn, Germany
February 2015	Workshop on Algebraic, Number Theoretic and Graph Theoretic Aspects of Dynamical Systems, UNSW, Sydney, Australia
November 2014	Number Theory Seminar, Max Planck Institute for Mathematics, Bonn, Germany
October 2014	Number Theory Seminar, UNSW, Sydney, Australia
July 2014	Oberseminar, B-IT CoSec, Bonn, Germany
July 2014	Seminar during the Dynamics and Numbers Program, Max Planck Institute for Mathematics, Bonn, Germany
June 2014	Workshop on the Occasion of Harald Niederreiter's 70th Birthday: Applications of Algebra and Number Theory, Linz, Austria
April 2014	Joint Colloquim, UNSW, Sydney, Australia
February 2014	Workshop on Unlikely Intersections, CIRM, Luminy, France
October 2013	Research Seminar, Bielefeld University, Germany
October 2013	Colloquium, University of Neuchatel, Switzerland
September 2012	Workshop on Finite Fields and Their Applications: Character Sums and Polynomials Strobl, Austria
July 2012	Third Workshop on Mathematical Cryptology, CIEM-Castro Urdiales, Spain
February 2012	10th International Conference on Monte Carlo and Quasi-Monte Carlo Methods in Scientific Computing, UNSW, Sydney, Australia
January 2012	Workshop on Permutation Polynomials over Finite Fields and their Applications, Sabanci University, Istanbul, Turkey
October 2011	Workshop on Rational Functions over Finite Fields and their Applications, Sabanci University, Istanbul, Turkey
October 2011	Research Seminar, The Erwin Schrödinger Intern. Institute for Mathematical Physics (ESI), Vienna, Austria
July 2011	The 10th International Conference on Finite Fields and their Applications, Ghent, Belgium
April 2011	Research Seminar on Coding Theory and Cryptography, NTU, Singapore
April 2011	Research Seminar of the Department of Mathematics, University of Cantabria, Spain
March 2011	Arithmetic, Geometry, Cryptography and Coding Theory, AGCT-XIII, CIRM, Luminy, France
December 2010	Workshop on Dynamical Systems and Number Theory, Macquarie University, Sydney
July 2010	International Conference on Uniform Distribution Theory, UDT-2010, Strobl, Austria

June 2010	WAIFI 2010, Istanbul
January 2010	Number Theory Colloquium, TU Graz
December 2009	Coding Theory and Cryptography Seminar, University of Basel
November 2007	Commutative Algebra Seminar, University of Zürich

Other conferences and workshops attended[2]

April 2022	Diophantische Approximationen, MFO, Germany
October 2020	Number Theory Down Under, University of Melbourne (online)
July 2020	Algorithmic Number Theory Symposium (ANTS XIV), University of Auckland (online)
April 2020	Diophantische Approximationen, MFO, Germany (cancelled due to COVID-19)
September 2019	Topics in Rational and Integral Points, Basel, Switzerland
March 2019	Hawaii Number Theory 2019 (HINT), Honolulu, USA
July 2017	Where Geometry meets Number Theory, Gothenburg, Sweden
July 2017	Specialization problems in Diophantine Geometry, Cetraro, Italy
February 2017	Workshop on Heights and Applications to Unlikely Intersections Fields Institute, Toronto, Canada
September 2015	Workshop Analytic Number Theory and Diophantine Geometry, Leibniz University, Hannover
July 2014	Pseudorandomness in Number Theory, CIRM, Luminy
July 2014	Dynamics and Numbers, Max Planck Institute for Mathematics, Bonn
February 2014	Prime Numbers: New Perspectives, CIRM, Luminy
July 2013	The 11th International Conference on Finite Fields and their Applications, Otto-von-Guericke-University Magdeburg
July 2012	Third International Conference on Symbolic Computation and Cryptography, CIEM-Castro Urdiales, Spain
March 2012	ICERM Semester Program on Complex and Arithmetic Dynamics ICERM, Brown University, USA
October 2011	Dynamics and Number Theory, ESI, Vienna, Austria
May 2010	Public Key Cryptography and the Geometry of Numbers, Amsterdam, Netherlands
April 2010	Computer Security and Cryptography, CRM, University of Montreal, Canada
January 2010	Workshop on Dynamical Systems and Uniform Distribution, TU Graz, Austria
May 2009	Retrospective Meeting in Cryptography, Fields Institute, Toronto, Canada
July 2008	S^3CM: Soria Summer School on Computational Mathematics, Soria, Spain
April 2008	New Challenges in Digital Communications, Vlora, Albania
March 2008	4th Workshop on Coding and Systems, Alicante, Spain

Publications

Edited Books

1. H. Niederreiter, A. Ostafe, D. Panario and A. Winterhof (Eds.), *Algebraic Curves and Finite Fields*, Radon Series on Computational and Applied Mathematics **16**, De Gruyter, 2014.

Preprints

2. A. Ostafe and I. Shparlinski, "Additive energy of cyclic matrix groups and character sums with matrix exponential functions", *Preprint* (*arXiv: 2108.13146*).

[2]The list excludes the workshops/conferences that I co-organised and the ones listed under the "Research Talks" section.

3. A. Bérczes, Y. Bugeaud, J. Mello, A. Ostafe and M. Sha, "Multiplicative dependence of rational values modulo approximate finitely generated groups ", *Preprint* (*arXiv: 2107.05371*).

4. A. Ostafe, "On a Problem of Lang for Matrix Polynomials", *Preprint* (*arXiv: 2105.07705*).

5. D. Ghioca, A. Ostafe, S. Saleh and I. E. Shparlinski, "On sparsity of representations of polynomials as linear combinations of exponential functions", *Submitted* (*arXiv: 2102.01949*).

6. R. Dietmann, A. Ostafe and I. Shparlinski, "Discriminants of fields generated by polynomials of given height", *Submitted* (*arXiv: 1909.00135*).

Refereed Journal Articles

7. F. Barroero, L. Capuano, L. Mérai, A. Ostafe and M. Sha, "Multiplicative and linear dependence in finite fields and on elliptic curves modulo primes", *Int. Math. Res. Not.*, in press (*arXiv: 2008.00389*).

8. A. Ostafe, L. Pottmeyer and I. Shparlinski, "Perfect powers in value sets and orbits of polynomials", *New York J. Math.*, in press (*arXiv: 1907.12057*).

9. D. Ghioca, A. Ostafe, S. Saleh and I. E. Shparlinski, "A sparsity result for the Dynamical Mordell-Lang Conjecture in positive characteristic", *Bull. Aust. Math. Soc.*, in press (*arXiv: 2012.13711*).

10. A. Ostafe and I. Shparlinski, "On the Skolem problem and some related questions for parametric families of linear recurrence sequences", *Canadian J. Math.*, in press (*arXiv: 2005.06713*).

11. L. Mérai, A. Ostafe and I. Shparlinski, "Dynamical irreducibility of polynomials in reduction modulo primes", *Mathematische Zeitschrift*, in press (*arXiv: 1905.11657*).

12. A. Bérczes, A. Ostafe, I. Shparlinski and J. H. Silverman, "Multiplicative dependence among iterated values of rational functions modulo finitely generated groups", *Int. Math. Res. Not.*, **12** (2021), 9045–9082.

13. A. Ostafe and M. Young, "On algebraic integers of bounded house and preperiodicity in polynomial semigroup dynamics", *Trans. Amer. Math. Soc.*, **373** (2020), 2191-2206.

14. A. Ostafe, M. Sha, I. Shparlinski and U. Zannier, "On multiplicative dependence of values of rational functions and a generalisation of the Northcott theorem", *Michigan Math. J.*, **68** (2019), 385–407.

15. C. D'Andrea, A. Ostafe, M. Sombra and I. Shparlinski, "Modular reduction of systems of polynomial equations and algebraic dynamical systems", *Trans. Amer. Math. Soc.* (2019), v. 371, 1169–1198.

16. A. Ostafe, "Polynomial values in affine subspaces of finite fields", *Journal d'Analyse Mathematique*, **138** (2019), 49–81.

17. C. D'Andrea, M.-C. Chang, A. Ostafe, M. Sombra and I. Shparlinski, "Orbits of polynomial dynamical systems modulo primes", *Proc. Amer. Math. Soc.* (2018), v.146 , 2015–2025.

18. A. Ostafe, M. Sha, I. Shparlinski and U. Zannier, "On abelian multiplicatively dependent points on a curve in a torus", *Quart. J. Math* (2018), v. 69, 391–401.

19. D. Gomez-Perez, A. Ostafe and M. Sha, "The arithmetic of consecutive polynomial sequences over finite fields", *Finite Fields and Their Appl.*, (2018), v. 50, 35–65.

20. A. Ostafe, "On roots of unity in orbits of rational functions", *Proc. Amer. Math. Soc.* (2017), v. 145, 1927–1936.

21. A. Ostafe, "On some extensions of the Ailon-Rudnick theorem", *Monatshefte für Mathematik* (2016), v. 181, 451–471.

22. D. Gomez-Perez, J. Gutierrez and A. Ostafe, "Common composites of triangular polynomial systems and hash functions", *J. Symb. Comp.* (2016), v. 72, 182–195.

23. A. Ostafe and M. Sha, "On the quantitative dynamical Mordell-Lang conjecture", *J. Number Theory* (2015), v. 156, 161–182. (Corrigendum, *J. Number Theory* (2016), v. 164, 433–437.

24. D. Gomez-Perez, A. Ostafe and A. Topuzoglu, "On the Carlitz rank of permutations of $\mathbb{F}_p$ and pseudorandom sequences", *J. Complexity* (2014), v. 30, 279-289.

25. D. Gomez-Perez, A. Ostafe and I. E. Shparlinski, "On irreducible divisors of iterated polynomials", *Revista Matemática Iberoamericana* (2014), v. 30, 1123–1134.

26. D. Gomez-Perez, A. P. Nicolás, A. Ostafe and D. Sadornil, "Stable polynomials over finite fields", *Revista Matemática Iberoamericana* (2014), v. 30, 523–535.

27. D. Gomez-Perez, A. Ostafe and I. E. Shparlinski, "Algebraic entropy, automorphisms and sparsity of algebraic dynamical systems and pseudorandom number generators", *Math. Comp.*, v. 83 (2014), 1535–1550.

28. J. Cilleruelo, M. Z. Garaev, A. Ostafe and I. E. Shparlinski, "On the concentration of points of polynomial maps and applications", *Mathematische Zeitschrift*, (2012), v. 272, 825–837.

29. O. Ahmadi, F. Luca, A. Ostafe and I. E. Shparlinski, "On stable quadratic polynomials", *Glasgow Math. J.* (2012), v. 54, 359–369.

30. A. Ostafe and I. E. Shparlinski, "On the power generator and its multivariate analogue", *J. Complexity* (2012), v. 28, 238–249.

31. A. Ostafe, "Pseudorandom vector sequences of maximal period generated by polynomial dynamical systems", *Designs, Codes and Cryptography* (2012), v. 63, 59–72.

32. A. Ostafe and I. E. Shparlinski, "Exponential sums over points of elliptic curves with reciprocals of primes", *Mathematika* (2012), v. 58, 21–33.

33. A. Ostafe and I. E. Shparlinski, "Multiplicative character sums and products of sparse integers in residue classes", *Period. Math. Hungarica* (2012), v. 64, 247–255.

34. S. R. Blackburn, A. Ostafe and I. E. Shparlinski, "On the distribution of the subset sum pseudorandom number generator on elliptic curves", *Unif. Distrib. Theory* (2011), v. 6, 127–142.

35. A. Ostafe and I. E. Shparlinski, "On the Waring problem with Dickson polynomials in finite fields", *Proc. Amer. Math. Soc.*, (2011), v.139, 3815–3820.

36. A. Ostafe, I. E. Shparlinski and A. Winterhof, "Multiplicative character sums of a class of nonlinear recurrence vector sequences", *Intern. J. Number Theory* (2011), v.7, 1557-1571.

37. A. Ostafe and I. E. Shparlinski, "Twisted exponential sums over points of elliptic curves", *Acta Arith.* (2011), v. 148, 77–92.

38. A. Ostafe and I. E. Shparlinski, "Pseudorandomness and dynamics of Fermat quotients", *SIAM J. Discr. Math.* (2011), v. 25, 50–71.

39. A. Ostafe, E. Pelican and I. E. Shparlinski, "On pseudorandom numbers from multivariate polynomial systems", *Finite Fields and Their Appl.* (2010), v.16, 320–328.

40. A. Ostafe, I. E. Shparlinski and A. Winterhof, "On the generalized joint linear complexity profile of a class of nonlinear pseudorandom multisequences", *Adv. in Math. of Communications* (2010), v.4, 369–379.

41. A. Ostafe and I. E. Shparlinski, "On the length of critical orbits of stable quadratic polynomials", *Proc. Amer. Math. Soc.* (2010), v. 138, 2653–2656.

42. A. Ostafe and I. E. Shparlinski, "Pseudorandom numbers and hash functions from iterations of multivariate polynomials", *Cryptography and Communications* (2010), v.2, 49–67.

43. A. Ostafe, "Multivariate permutation polynomial systems and nonlinear pseudorandom number generators", *Finite Fields and Their Appl.* (2010), v. 16, 144–154.

44. A. Ostafe and I. E. Shparlinski, "On the degree growth in some polynomial dynamical systems and nonlinear pseudorandom number generators", *Math. Comp.* (2010), v. 79, 501–511.

45. R. Ferguson, C. Hoffman, F. Luca, A. Ostafe and I. E. Shparlinski, "Some additive combinatorics problems in matrix rings", *Revista Matematica Complutense*, (2010), v.23, 501–513.

Book Chapters

46. A. Ostafe and I. E. Shparlinski, "Orbits of Algebraic Dynamical Systems in Subgroups and Subfields", *Number Theory - Diophantine problems, uniform distribution and applications*, Festschrift in Honour of Robert F. Tichy's 60th Birthday, Springer, 2017, 347–368.

47. A. Ostafe and M. Sha, "Counting dynamical systems over finite fields", *Dynamics and Numbers 2014*, Contemp. Math. (2016), v. 669, 187–203.

48. A. Ostafe, "Iterations of rational functions: some algebraic and arithmetic aspects", *Finite Fields and Their Applications. Character Sums and Polynomials*, De Gruyter, 2013, 197–232.

49. A. Ostafe and A. Winterhof, "Some applications of character sums", *Handbook of Finite Fields*, CRC Press, Eds. G. Mullen and D. Panario, 2013, 170–185.

50. A. Ostafe, D. Thomson and A. Winterhof, "On the Waring problem with multivariate Dickson polynomials", *Finite fields and Applications*, Contemp. Math., (2012), v. 579, 153–161.

51. A. Ostafe and I. E. Shparlinski, "Degree growth, linear independence and periods of a class of rational dynamical systems", *Arithmetic, Geometry, Cryptography and Coding Theory 2010*, Contemp. Math., (2012), v. 574, 131–143.

Refereed Conference Papers

52. Z. Chen, A. Ostafe and A. Winterhof, "Structure of pseudorandom numbers derived from Fermat quotients", *Proc. Intern. Workshop on the Arith. of Finite Fields, Istanbul, WAIFI 2010*. Lect. Notes in Comp. Sci., vol. 6087, Springer-Verlag, Berlin, 2010, 73–85.

53. A. Ostafe, "Pseudorandom vector sequences derived from triangular polynomial systems with constant multipliers", *Proc. Intern. Workshop on the Arith. of Finite Fields, Istanbul, WAIFI 2010*. Lect. Notes in Comp. Sci., vol. 6087, Springer-Verlag, Berlin, 2010, 62–72.