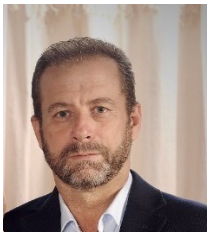
Tony Shaska Sr.

Department of Mathematics and Statistics
Oakland University
Rochester, MI 48309
Phone: 248-760-7447
E-mail: tanush@umich.edu, shaska@oakland.edu
Webpage: www.risat.org/shaska.html



Research areas

Computational Algebraic and Arithmetic Geometry, *Computational algebra*, algebraic geometry, number theory, algebraic curves, arithmetic in moduli spaces, weighted projective spaces, weighted heights, minimal models of curves, machine learning in moduli spaces, arithmetic dynamics, etc.

Cybersecurity and Data Protection, *Elliptic (ECC), Hyperelliptic Curve Cryptography (HCC), Isogeny based post-quantum cryptography*.

Machine Learning and Artificial Intelligence, *NLP, computational linguistics, social intelligence*, AI-enabled cultural interpreters or Multicultural AI, Automated Theorem Proving.

Education

May 2001 **Doctor of Philosophy**, *Mathematics*, The University of Florida, Gainesville, FL.
Thesis: Curves of genus two covering elliptic curves

May1998 **Masters of Science**, *Mathematics*, The University of Florida, Gainesville, FL.

Dec. 1994 **Bachelor of Science**, *Mathematics*, University of Michigan (Highest Distinction).
Major: Mathematics; **Minor:** Computer Science, **GPA:** 3.95/4.0, Major GPA: 4.0/4.0

Experience

Aug. 2007-current **Associate Professor**, *Department of Mathematics and Statistics, Oakland University, MI.*
Created most of the graduate algebra curriculum including new courses in commutative ring theory, algebraic number theory, algebraic geometry and supervised several PhD students.

Aug.23 - Dec. 23 **Visiting Scholar**, *Department of Mathematics*, University of Michigan, Ann Arbor.

Jan.15 - May 15 **Visiting Professor**, *Department of Mathematics*, Princeton University.

Mar. 11-current **Co-founder, Senior Researcher, and Trustee**, *Research Institute of Science and Technology*.
A non-profit international scientific institute with activities in SouthEastern Europe and Mediterranean countries focused in mathematics, computer science, cybersecurity.

Jan.08 -Dec.10 **Rector**, *University of Vlora*, Vlora, Albania.
As Rector I served as CEO/CFO and Chief Academic Officer of the University, which at the time went through the biggest expansion in its history. During my tenure University of Vlora achieved the highest ranking of any university in Balkans and started new undergraduate and graduate programs in all STEM fields.

Jan.08 - current **Professor of Mathematics**, *Ministry of Education and Sciences*, Albania.

Jan. 07-current **Founding Editor and Editor in Chief**, *Albanian Journal of Mathematics*.
Founder of the Albanian Journal of Mathematics. I have served as Editor in Chief for the journal, which publishes regularly for the last two decades.

Aug.05-Aug.07 **Assistant Professor**, *Department of Mathematics and Statistics, Oakland University, MI.*

Aug.03-Jun.05 **Assistant Professor of Mathematics**, *University of Idaho*, Moscow, ID.

Aug.01-Jun.03 **Visiting Assistant Professor**, *Department of Mathematics, UC–Irvine, CA*.
Worked under the direction of Mike Fried in the Department of Mathematics at UC-Irvine

Jan.00 -Aug.00 **Universität Erlangen-Nürnberg**, *DFG Fellowship*, Erlangen, Germany.
I spent most of my 4th year of graduate study as a DFG fellow in Erlangen Germany.

Aug.96-May.01 **Graduate Teaching Assistant**, *Department of Mathematics*, University of Florida, Gainesville, FL.
Taught most of the freshmen courses in mathematics.

Jan.95-Aug.96 **Programer/Consultant**, *Computer Business Solutions Inc., Farmington Hills, MI.*
AS 400, Unix, C, C++, SQL, Oracle, etc.

Awards and Grants

2024 **Nato Science for Piece and Security Grant**, *Quantum-resistant cryptography (QsafeCrypt)*, NATO countries: France, Romania, United States, NATO Partner Countries: Morocco (pending). G. Hains, M. Hedabou, T. Shaska, V. Niculescu

2024 **Nato Science for Piece and Security Grant**, *Isogeny based post-quantum cryptography*. Co-Pi: Shaul Zemel, The Hebrew University of Jerusalem

2014 **Nato Advanced Study Institute**, *Hyperelliptic Curve Cryptography*, ISEG. EAP.ASI 984724. Co-Pi: Eustrat Zhupa, Department of Computer Science, University of Rochester

2012 **National Security Agency**, *East Coast Computer Algebra Day*, NSA: #H982301210275.

2007-2010 **National Science Foundation**, *REU*, Oakland University, Co-PI.

2008 **Nato Advanced Study Institute**, *New challenges in digital communications*, ICS.EAP.ASI 982903.

2007 **National Science Foundation**, *Applications of Computer Algebra*, Oakland University.

2005 **National Security Agency**, *Computational Aspects of Algebraic Curves, Univ. of Idaho.*

2004 **National Science Foundation**, *NSF-Epscor S0-511*, University of Idaho, NSF.

2000 **Deutsche Forschungsgemeinschaft**, *Friedrich-Alexander-Universität Erlangen-Nürnberg*.

2001 **Threadgill Dissertation Award**, *Department of Mathematics*, University of Florida.

Dec. 1994 **Graduated with Highest Distinction**, *University of Michigan*.

Long term visits

Fall 23 **Department of Mathematics, University of Michigan**, *Ann Arbor, MI*, sabbatical.

Summer 22 **Research Institute of Science and Technology**, *Vlora*, Albania.

October 21 **Universidad de Cantabria-Santander**, *Spain*.

Summer 21 **Research Institute of Science and Technology**, *Vlora*, Albania.

Winter 15 **Department of Mathematics, Princeton University**, *Princeton, NJ*, sabbatical.

June 13 **Linkoping University**, *Linkoping*, Sweden.

Summer 12 **Visiting Professor**, *University of Pristina*, Pristina, Kosova.

Nov. 10 **Mathematical Sciences Research Institute**, *Berkeley, CA.*. Workshop on Hybrid Methodologies for Symbolic-Numeric Computation

Oct. 09 **Universidad de Cantabria-Santander**, *Spain*.

Summer 07 **Visiting Professor**, *Maria Curie-Sklodowska University*, Lublin, Poland.

Sep. 06 **Institute of Mathematics and Applications (IMA)**, *University of Minnesota*, Algorithms in Algebraic Geometry, Organizers: Alicia Dickenstein, Frank-Olaf Schreyer, Andrew Sommese.

Summer 2006 **Institut für Experimentelle Mathematik**, *Essen*, Germany.

Aug. 05 **Institute of Mathematics and Applications (IMA)**, *Quantum Computation*, Minnesota.

Dec. 04 **Institut für Experimentelle Mathematik**, *Essen*, Germany.

Summer 03 **Universidad de Cantabria-Santander**, *Spain*.

Summer 03 **Institut für Experimentelle Mathematik**, *Essen*, Germany.

Jul. 02 **University of Sydney**, *Sydney*, Australia.

Jun. 01 **Universität Erlangen-Nürnberg**, *Erlangen*, Germany.

Summer 01 **Institut für Experimentelle Mathematik**, *Essen*, Germany.

Dec. 00 **Mathematical Sciences Research Institute**, *Arithmetic Geometry*. Organizers: Noam Elkies, William McCallum, Jean-François Mestre, Bjorn Poonen, and René Schoof

Jan.-Aug. 00 **Universität Erlangen-Nürnberg**, *DFG Fellowship*, Germany.

Fall 99 **Mathematical Sciences Research Institute**, *Berkeley, CA*, Galois Groups and Fundamental Groups, Organizers: E. Bayer, M. Fried, D. Harbater, Y. Ihara, H. Matzat, M. Raynaud, J. Thompson.

June 99 **Institute for Advanced Study/Park City Institute**, *Arithmetic Geometry*, Park City, Utah.

Summer 98 **IWR**, *University of Heidelberg*, Heidelberg, Germany.

Computer Skills

Unix, C, C++, SQL, Oracle, Python, Pytorch, Tensorflow, GAP, Sagemath, Maple, Mathematica

Editorial

2024 **Isogeny based post-quantum cryptography**, *NATO Science for Peace and Security Series - D: Information and Communication Security*, Shaska/Zemel, (to appear).

2024 **Recent advances in mathematics and artificial intelligence**, *Cont. Math.*, to appear.

2021 **Abelian varieties and number theory**, *Cont. Math.*, Frey's 75th birthday, Jarden/Shaska.

2020 **Integrable systems and Algebraic Geometry**, *Vol 1, Cambridge Univ. Press,* , Donagi/Shaska.

2020 **Integrable systems and Algebraic Geometry**, *Vol. II, Cambridge Univ. Press,*, Donagi/Shaska.

2019 **Algebraic curves and their applications**, *Cont. Math. Volume: 724; 19; 344 pp;*, Beshaj/Shaska.

2018 **Higher Genus Curves in Mathematical Physics and Arithmetic Geometry**, *Cont. Math. (703), 18. vii+222 pp.*, Malmendier/Shaska.

2015 **Advances on superelliptic curves and their applications**, *NATO Science for Peace and Security Series - D: Information and Communication Security, Vol 41. 15*, Beshaj/Shaska/Zhupa.

2013 **Computational algebraic geometry & applications**, *Appl. Alg. Eng. Comm. Comp.*, vol. 24.

2013 **Computational Algebraic Geometry**, *J. Symbolic Comp.*, Vol. 57, 2013, 1-78..

2009 **Algebraic Aspects of Digital Communications**, *NATO Science for Peace and Security Series, D: Information and Communication Security*, Vol. 24. viii+285 pp.

2007 **Coding theory and cryptography**, *Serdica J. Comput.*, Vol. I, No. 2, 07.

2007 **Advances in coding theory and cryptology**, *Series: Coding Theory and Cryptography, Vol. 3, World Scientific Publishing,*, Huffman/Joyner/Shaska/Ustimenko.

2005 **Computational aspects of algebraic curves**, *Lecture Notes in Comp., World Scientific, vol. 13*, World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2005. xii+272 pp. ISBN: 981-256-459-4.

2005 **Progress in Galois Theory**, *Proceedings of John Thompson's 70th Birthday Conference held at the University of Florida, Gainesville, FL, November 4?8, 2002.*, Dev. Math. 12, Völklein/Shaska.

Papers

Submitted or in preparation

71. A machine learning approach of Julia reduction(in progress)
70. Deep learning and the moduli space of curves
69. Automorphism groups of rational functions
68. Vojta's conjecture on weighted projective varieties
67. Arithmetic inflection of superelliptic curves
66. On generalized superelliptic Riemann surfaces

Selected journal articles

65. Local and global heights on weighted projective varieties, S. Salami and T. Shaska, *Houston J. Math.* (to appear)
64. A. Clingher, A. Malmendier, T. Shaska; On isogenies among certain Abelian varieties, *Mich. Math. J.*, 71, No. 2, 227-269 (2022).
63. A. Clingher, A. Malmendier, T. Shaska; Geometry of Prym varieties for special bielliptic curves of genus three and five, Pure Appl. Math. Q. 17, No. 5, 1739-1784 (2021).
62. A. Obus, T. Shaska; Superelliptic curves with many automorphisms and CM Jacobians, *Math. Comp.,* **90**, (2021), 332, 2951–2975.
61. A. Elezi, T. Shaska; Reduction of binary forms via the hyperbolic centroid, *Lobachevskii J. Math.* **42**, (2021), 1, 84–95.
60. L. Beshaj, A. Elezi, T. Shaska;Isogenous components of Jacobian surfaces, *Eur. J. Math.* **6**, (2020), no. 4, 1276–1302.
59. L. Beshaj, J. Gutierrez, T. Shaska; Weighted greatest common divisors and weighted heights, *J. Number Theory*, 213 (2020), 319-346.
58. A. Clingher, A. Malmendier, T. Shaska; Six line configurations and string dualities, *Commun. Math. Phys.*, (2019) 371, 159-196.

57. A. Malmendier, T. Shaska; From hyperelliptic to superelliptic curves, Albanian J. Math., **13**, (2019), No. 1,107-200.

56. Shuichi Otake, Tony Shaska; Some remarks on the non-real roots of polynomials, Cubo, **20**, (2018) no. 2, 67-93.

55. Gerhard Hiss, Tony Shaska;Kay Magaard (1962–2018), Special issue in honor of Kay Magaard, Albanian J. Math. Vol. 12 2018, no. 1, 33-35.

54. A. Malmendier, T. Shaska; A universal pair of genus-two curves from Siegel modular forms, SIGMA. Symmetry, Integrability and Geometry. Methods and Applications 13, (2017), 089, 17 pages

53. A. Malmendier, T. Shaska; The Satake sextic in F-theory, Journal of Geometry and Physics vol. 120, (2017), 290-305

52. T. Shaska, C. Shor 2-Weierstrass points of genus 3 hyperelliptic curves with extra automorphisms, Comm. in Algebra 45 (2017), no. 5, 1879 - 1892.

51. T. Shaska; Genus two curves with many elliptic subcovers, Comm. in Algebra 44 (2016), Nr. 10, 4450-4466

50. T. Shaska, C. Shor Theta functions and complete weight enumerators for codes over imaginary quadratic fields, Des. Codes Cryptogr. vol 76, 2015, 217-235

49. T. Shaska, F. Thompson Bielliptic curves of genus 3 in the hyperelliptic moduli, Appl. Algebra Engrg. Comm. Comput. Volume 24, 2013, 387-412

48. T. Shaska; Some remarks on the hyperelliptic moduli of genus 3, Communications in Algebra 42 (9), 2014, 4110–4130

47. A. Elezi, T. Shaska; Quantum codes from superelliptic curves Albanian J. Math. Vol. 5. Nr. 4, 2011, pg. 175–191

46. L. Beshaj, V. Hoxhaj, T. Shaska; On superelliptic curves of level n and their quotientsAlbanian J. Math., Vol. 5. Nr. 3, pg. 115-138, 2011

45. T. Shaska, C. Shor, G. Wijesiri Codes over rings of size p^2 and lattices over imaginary quadratic fields, Finite Fields Appl. 16 (2010), no. 2, 75–87

44. K. Magaard, T. Shaska, H. Voelklein Genus 2 curves that admit a degree 5 map to an elliptic curve, Forum Math. 21, (2009), no. 3, 547–566

43. T. Shaska, V. Ustimenko On the homogeneous algebraic graphs of large girth and their applications, Linear Algebra Appl. 430 (2009), no. 7, 1826–1837

42. T. Shaska, V. Ustimenko On some applications of graphs to cryptography and turbocoding, Albanian J. Math.,Vol 2, Nr. 3, 2008, 249 – 255.

41. N. Pjero, M. Ramosaco, T. Shaska; Degree even coverings of elliptic curves by genus two curves, Albanian J. Math.vol. 2. Nr. 3, 2008, 241-248

40. T. Shaska; Quantum codes from algebraic curves with automorphisms, Condensed Matter Physics Vol. 11, 2008, No 2 (54), 383-396.

39. T. Shaska, R. Sanjeewa Determining equations of families of cyclic curves, Albanian J. Math. Vol 2, Nr. 3, 2008, 199-213

38. T. Shaska, G. Wijesiri, S. Wolf, S. Woodland Degree four coverings of elliptic curves by genus two curves, Albanian J. Math. vol. 2. Nr. 4. 2008, 307-318

37. T. Shaska, G. Wijesiri Codes over rings of size four, Hermitian lattices, and corresponding theta functions, Proc. Amer.Math. Soc. 136 (2008), no.3, 849-857

36. E. Previato, T. Shaska, G. WijesiriThetanulls of cyclic curves of small genus, Albanian J. Math. vol. 1, Nr. 4, 2007, 253-270

35. T. Shaska;Some open problems in computational algebraic geometry, Albanian J. Mathvol I, Nr. 3, 07, 297-319

34. T. Shaska, Q. Wang; Automorphism groups of AG-codes based on C_{ab} curves, *Serdica J. Comp.*, Vol.1 (2007), 193-206

33. T. Shaska; Hyperelliptic curves with reduced automorphism group A_5, Appl. Algebra Engrg. Comm. Comput. vol. 18, Nr. 1-2, 2007, pg. 3-20

32. T. Shaska, Subvarieties of hyperelliptic moduli determined by group actions, *Serdica Math. Jour.* **4** (2006), 355-374

31. J. Gutierrez, T. Shaska; Hyperelliptic curves with extra involutions, LMS J. of Comp. Math. 8, (2005), 102-115.
30. T. Shaska;Some special families of hyperelliptic curves, J. Algebra Appl. 3 (2004), no. 1, 75–89
29. T. Shaska; Genus 2 fields with degree 3 elliptic subfields, Forum Math. 16 (2004), no. 2, 263–280
28. K. Magaard, T. Shaska, S. Shpectorov, H. Völklein; The locus of curves with prescribed automorphism group, Sūrikaisekikenkyūsho Kōkyūroku No. 1267 (2002), 112–141
27. T. Shaska; Curves of Genus 2 with (n, n)-decomposable Jacobians, Jour. Symb. Comp. vol.31 (2001), No.5, 603-617.

Reviewed Conference Proceedings

26. T. Shaska; Reduction of superelliptic Riemann surfaces Automorphisms of Riemann surfaces, subgroups of mapping class groups and related topics, 227 – 247, Contemp. Math., 776, Amer. Math. Soc., (2022).
25. G. Frey and T. Shaska; Curves, Jacobians, and Cryptography Contemporary Math. vol. 724, 19, pg. 279-345.
24. A. Broughton, A. Wootton, T. Shaska; On automorphisms of algebraic curves Contemporary Math. vol. 724, 19, pg. 175-212.
23. Shuichi Otake and Tony Shaska; Bezoutians and the discriminant of a certain quadrinomials Contemporary Math. vol. 724, 19, pg. 55-72.
22. J. Mandili and T. Shaska; Heights on weighted projective spaces Contemporary Math. vol. 724, 19, pg. 149-160.
21. R. Hidalgo and T. Shaska; On the field of moduli of superelliptic curves Contemporary Math. vol. 703, 18, 49-64
20. L. Beshaj, R. Hidalgo, A. Malmendier, S. Kruk, S. Quispe, T. Shaska; Rational points on the moduli space of genus two Contemporary Math. vol. 703, 18, 87-120
19. D. Joyner, T. Shaska; Self-inversive polynomials, curves, and codes Contemporary Math. vol. 703, 18, 197 - 218
18. L. Beshaj, A. Elezi, T. Shaska; Theta functions of superelliptic curves Information security, coding theory and related combinatorics NATO Sci. Peace Secur. Ser. D Inf. Commun. Secur., 29, IOS, 15, 47–69
17. A. Elezi, T. Shaska; Weight distributions, zeta functions and Riemann hypothesis for linear and algebraic geometry codes Information security, coding theory and related combinatorics NATO Sci. Peace Secur. Ser. D Inf. Commun. Secur., 29, IOS, 15, 259–298
16. M. Izquierdo, T. Shaska; Cyclic curves over the reals Information security, coding theory and related combinatorics, 59–98 NATO Sci. Peace Secur. Ser. D Inf. Commun. Secur., 39, IOS, Amsterdam, 15.
15. L. Beshaj and T. Shaska; Heights on algebraic curves Information security, coding theory and related combinatorics, 159–198 NATO Sci. Peace Secur. Ser. D Inf. Commun. Secur., 29, IOS, Amsterdam, 11.
14. L. Beshaj and T. Shaska; Decomposition of some Jacobian varieties of dimension 3 Artificial Intelligence and Symbolic Computation LNCS vol. 8884, 193-204
13. L. Beshaj, T. Shaska, C. Shor On Jacobians of curves with superelliptic components Contemp. Math. vol. 29, 14, 1–14
12. L. Beshaj and T. Shaska; The arithmetic of genus 2 curves Information security, coding theory and related combinatorics 59–98, NATO Sci. Peace Secur. Ser. D Inf. Commun. Secur., 29, IOS, Amsterdam, 2011.
11. T. Shaska and G. Wijesiri Theta functions and algebraic curves with automorphisms Algebraic aspects of digital communications, NATO Sci. Peace Secur. Ser. D Inf. Commun. Secur., 24 IOS, Amsterdam, 2009, 193 – 237
10. T. Shaska and C. Shor Codes over F_{p^2} and $F_p \times F_p$, lattices, and theta functions Advances in Coding Theory and Cryptology vol 3. (2007), pg. 70-80
9. A. Bialostocki and T. Shaska; Galois groups of prime degree polynomials with nonreal roots Lect. Notes in Computing 13, 2005, 243–255
8. J. Gutierrez, T. Shaska, D. Sevilla Hyperelliptic curves of genus 3 with prescribed automorphism groups Lect. Notes Comp. vol 13. (2005), 109–123
7. V. Krishnamoorthy, T. Shaska, H. Voelklein Invariants of binary forms Dev. in Math. vol 12, pg.101-122, Springer, 05

6. T. Shaska; Genus 2 curves covering elliptic curves: a computational approach Lect. Notes in Comp. vol 13. (2005), 205-231
5. T. Shaska; Computational Aspects of Hyperelliptic Curves Computer Mathematics Lecture Notes Ser. Comput. 10, 248–257, World Sci. Publishing, River Edge, NJ.
4. T. Shaska and J. Thompson; On the generic curve of genus 3 Contemporary Math. vol. 369, pg. 233-244, (American Math. Soc.), 2005
3. T. Shaska and H. Voelklein; Elliptic subfields and automorphisms of genus 2 function fields Algebra, arithmetic and geometry with applications Springer, 04, 703–723
2. T. Shaska; Determining the automorphism group of a hyperelliptic curve International Symposium on Symbolic and Algebraic Computation ISSAC 03, New York, 03, 248–254
1. T. Shaska; Genus 2 curves with $(3,3)$-split Jacobian and large automorphism group, Algorithmic number theory (Sydney, 2002) Lecture Notes in Comput. Sci., 2369, 205–218

Conferences Organized

May 2024 **Isogeny based postquantum cryptography**, *Jerusalem, Israel*, with Shaul Zemel.
July 2023 **Algebraic Aspects of Postquantum Cryptography**, *Warsaw, Poland.*
Jan. 2023 **Excursions in Arithmetic Geometry**, *Special session*, Joint Mathematics Meetings, Boston.
June 2022 **Recent trends in algebra, geometry, and arithmetic**, Vlora, Albania (with Elira Curri).
Mar. 2022 **Curves, Jacobians, and Abelian Varieties**, *AMS Sectional Meeting*, University of Virginia, with A. Obus and P. Srinivasan.
Jan. 2021 **Algebraic and Arithmetic Geometry**, *Joint Mathematics Meetings*, Washington, DC.
Mar. 2020 **Cyber defense and cryptography in undergraduate education**, *AMS Meeting*, Charlottesville.
Mar. 2020 **Curves, Jacobians, and Abelian Varieties**, *AMS Meeting*, Univ. of Virginia, Charlottesville, VA.
Dec. 2018 **Tirana Winter School in Algebraic Geometry**, *Tiranë*, Albania.
Oct. 2018 **From hyperelliptic to superelliptic curves**, *AMS Meeting*, Ann Arbor, MI.
Aug. 2018 **Algebraic Curves, Integrable Systems, Cryptography**, *Kiev*, (J. Bernatska and V. Enolski).
Mar. 2018 **Arithmetic of Algebraic Curves**, *AMS Meeting*, Columbus, OH, with A. Elezi and M. Polak.
Jan. 2017 **Minimal integral models of algebraic curves**, *AMS Joint Meeting*, Atlanta, GA.
Nov. 2016 **Varieties, their fibrations and automorphisms in mathematical physics and arithmetic geometry**, *AMS Sectional Meeting*, Raleigh, NC.
Jan. 2016 **Higher Genus Curves and Fibrations of Higher Genus Curves in Mathematical Physics and Arithmetic Geometry**, *Joint Mathematics Meetings AMS & MAA*, Seattle, WA.
Mar. 2015 **Arithmetic of Hyperelliptic Curves**, *Special Session*, AMS Meeting, East Lansing, MI.
Aug. 2014 **Nato Advanced Study Institute**, *Arithmetic of Hyperelliptic Curves*, Ohrid, Macedonia.
July 2014 **Applications of Computer Algebra**, *Fordham University*, New York, with R. H. Lewis.
July 2014 **Moduli spaces and arithmetic dynamics**, *Applications of Computer Algebra*, Fordham, NY.
July 2013 **Arithmetic of algebraic curves**, *Applications of Computer Algebra*, Malaga, Spain.
June 2012 **Michigan Computational Algebraic Geometry**, *Rochester, MI.*
June 2012 **East Coast Computer Algebra Day**, *Oakland University*, Rochester, MI, with D. Steffy.
Mar. 12 **Computational Algebraic Geometry**, *AMS Sectional Meeting*, Tampa, FL.
Jan. 2011 **Computational Algebraic and Analytic, Geometry for Low-Dimensional Varieties.**, *AMS Annual Meeting*, New Orleans.
June 2010 **Applications of Computer Algebra**, *Vlora*, Albania.
Jan. 2009 **Computational Algebraic and Analytic, Geometry for Low-Dimensional Varieties**, *AMS Annual Meeting*, Washington DC, with M. Seppala, E. Volchek.
May 2008 **Nato Advanced Study Institute**, *New challenges in digital communications*, Vlora, Albania.
May 07 **Conference in algebra, coding theory, and cryptography**, *Vlora, Albania*, A. Elezi, T. Shaska.
July 2007 **Applications of Computer Algebra**, *Rochester, MI.*
July 2007 **Coding theory and cryptography**, *Applications of Computer Algebra*, Special session, Rochester, MI, with D. Joyner, C. Shor.
Jul. 07 **Special session: Computational algebraic geometry**, *ACA 07, Rochester, MI.*

Jan. 2007 **Computational Algebraic and Analytic, Geometry for Low-Dimensional Varieties**, *AMS Annual Meeting*, New Orleans.

June 2006 **Coding theory and cryptography**, *Special Session*, Applications of Computer Algebra, Varna, Bulgaria, with S. Dodunekov.

May 2005 **Computational aspects of algebraic curves**, *University of Idaho*, Moscow, Idaho.

Jan. 2005 **Algorithmic Algebraic and Analytic Geometry**, *Special Session*, AMS Annual Meeting, Atlanta.

July 2004 **Computational aspects of algebraic curves**, Applications of Computer Algebra, Beaumont, TX.

July 2003 **Computational aspects of algebraic curves**, Applications of Computer Algebra, Raleigh, NC.

Sep. 2001 **Progress in Galois Theory**, *John Thompson's 70th birthday*, University of Florida, with H. Völklein.

Selected talks

April 24 **Machine Learning And Julia Invariant**, *AMS Special Session on Artificial Intelligence in Mathematics*, Milwaukee.

April 24 **Automorphism loci of rational functions of the projective line**, *AMS Special Session on Automorphisms of Riemann Surfaces and Related Topics*, Milwaukee.

Feb. 24 **A mini course in Machine Learning**, *Institute of Mathematics and Statistics*, State University of Rio de Janeiro, RJ, Brazil.

April 23 **Machine Learning and Moduli Spaces**, *Polynomial Computer Algebra 2023*, Euler International Mathematical Institute, St. Petersburg, Russia, (online).

April 23 **Machine learning in the moduli space of curves**, *University of Pristina, Kosova.*

April 23 **Genus two curves with (n, n)-split Jacobians**, *AMS Special Session on Cybersecurity and Cryptography*, Spring Eastern Sectional Meeting.

Mar.23 **Arithmetic geometry and its applications to cryptography**, *University of Alabama Huntsville.*

Feb. 23 **Arithmetic in the moduli space of curves**, *University of Nevada, Las Vegas.*

Sep. 22 **Arithmetic of algebraic curves and weighted heights**, *Izmir Yuksek Teknoloji Enstitusu, Turkie.*

May 22 **Local and global heights on weighted varieties and Vojta's conjecture**, *Vlora, AL.*

Mar. 20 **Computation on moduli spaces: an introduction to weighted moduli heights**, *AMS Meeting*, Moduli of Curves, Hilbert Schemes, and Tropical Geometry, Medford, MA.

Dec. 19 **Heights on weighted projective varieties**, *Mathematics Colloquium, University of Sarajevo.*

Oct. 19 **Addition on Jacobians from a geometric viewpoint**, *National University of Greece, Athens.*

Apr. 19 **Abelian varieties with complex multiplication**, *Explicit Methods on Abelian and Calabi-Yau varieties*, Utah State University, Logan.

Apr. 19 **Isogenies of 2-dimensional Jacobians**, *Mathematical Cryptology, AMS Meeting, Hartford, CT.*

Mar. 19 **Curves, automorphisms, and their Jacobians**, *Algebra seminar, College of Charleston, SC.*

Feb. 19 **CM Superelliptic curves**, *Annual Meeting of Spanish Math. Soc.*, Santander.

Nov. 18 **Heights on weighted projective spaces**, *Algebra Seminar, Wayne State University, Detroit, MI.*

Oct. 18 **Heights on weighted spaces**, *From hyperelliptic to superelliptic curves*, AMS Session, Ann Arbor.

Aug. 18 **Abelian Varieties and Cryptography**, *Algebraic Curves, Integrable Systems, and Cryptography, National University of Kyiv-Mohyla Academy, Kiev, Ukraine.*

Apr. 18 **The group law for the Jacobi variety of a hyperelliptic curves**, *Utah State, Logan, UT.*

Apr. 18 **Riemann surfaces with extra automorphisms and endomorphism rings of their Jacobians**, *Automorphisms of Riemann Surfaces and Related Topics, AMS Meeting, Portland, OR.*

Mar. 18 **Isogenies of Abelian varieties**, *Algebraic curves and applications, AMS Meeting*, Columbus, OH.

Sep. 17 **From hyperelliptic to superelliptic curves**, *Algebraic curves and applications, AMS Meeting*, University of Central Florida, Orlando, FL.

Apr. 17 **From hyperelliptic to superelliptic curves**, *Department of Mathematics, US Naval Academy.*

Jan. 16 **A pair of universal curves of genus 2**, *AMS Joint Meeting in Atlanta, GA.*

Oct. 15 **Theta functions and symmetric weight enumerators for codes over imaginary quadratic fields**, *AMS Session on Coding Theory and Its Applications, Chicago.*

Oct. 15 **Julia quadratic of superelliptic Riemann surfaces**, *AMS Meeting, Chicago.*

Jun. 15 **Integral minimal models for binary forms**, *Mathematics Colloquium, Gainesville.*

Mar. 15 **Binary forms of minimal height**, *AMS Sectional Meeting, East Lansing.*

Jul. 14 **Heights on algebraic curves**, *NATO Advanced Study Institute, Ohrid.*

Jul. 14 **Minimal models for curves over their minimal field of definition**, *App. Comp. Algebra, NY.*

Jul. 14 **Genus 3 hyperelliptic curves with (2, 4, 4) split Jacobians**, *App. Comp. Algebra, 2014, NY.*

Mar. 14 **Minimal equations of curves over their minimal field of definition**, *AMS Meeting, Knoxville.*

Jun. 13 **Decomposition of Jacobians of superelliptic curves**, *Riemann and Klein Surfaces, Symmetries and Moduli Spaces*, Linkoping, Sweden.

Apr. 13 **Automorphisms of curves and their Jacobians**, *Computational Advances on Special Functions and Tropical Geometry*, AMS Meeting, Iowa State.

May 13 **Stratifications on moduli spaces of curves and superelliptic loci**, *Michigan Computational Algebraic Geometry, MCAG 13*, Western Michigan University.

Mar. 13 **Genus 3 hyperelliptic curves with split Jacobians**, *Math. Colloquium, Georgia Southern.*

Nov. 12 **Some remarks on binary octavics**, *Mathematics Colloquium*, Michigan Tech. University.

Nov. 12 **Some remarks on binary octavics**, *Mathematics Colloquium*, Cleveland State University.

Oct. 12 **An introduction to the invariant theory of binary forms**, *Math. Colloquium*, Duquesne Univ..

Jun. 12 **Theta functions**, *Conference on Applications of Algebra*, Yildiz University, Istanbul, (plenary talk).

Mar. 12 **Thetanulls of curves and applications**, *AMS Session: Computational Algebraic Geometry, Tampa.*

Jan 12 **Interesting families of algebraic curves**, *Mathematics of Computation, AMS Meeting, Boston.*

Jan. 12 **Half-integer theta-nulls of superelliptic curves**, *Computational and Algorithmic Algebraic Geometry, AMS Meeting, Salt Lake, UT.*

Oct. 11 **Theta Functions of algebraic curves**, *SIAM National Conference, Raleigh, NC.*

Jul. 11 **Computational aspects of low genus curves**, *Laurier Centennial Conference: AMMCS-11, Waterloo.*

May 11 **Theta-nulls of algebraic curves**, *10th Panhellenic Geometry Conference, Patras, Greece.*

Nov. 10 **Hybrid Methodologies for Symbolic-Numeric Computation**, *MSRI, Berkeley.*

Oct. 09 **Automorphism groups of superelliptic curves**, *Math. Cryptology, Santander, Spain.*

Mar. 08 **Theta functions in coding theory**, *Mathematics Colloquium, University of Delaware.*

Oct. 07 **Genus 2 curves covering elliptic curves**, *Math. Colloquium, Simon Fraser Univ., Vancouver.*

Oct. 07 **Equations of curves with automorphisms**, *AMS Meeting: Numerical and Symbolic Techniques in Algebraic Geometry and Its Applications, DePaul University.*

Sep. 07 **Remarks on some old problems of algebraic geometry**, *Math. Colloquium, Michigan Tech..*

May 07 **A historical view of theta functions**, *Math. Colloquium, Lublin, Poland.*

Aug. 06 **Codes over rings of size four, lattices, and theta functions**, *Math. Colloquium, Lublin, Poland.*

May 06 **Theta functions and automorphism groups of curves**, *Galoistheorie Kolloquium, Institut für Experimentelle Mathematik, Essen, Germany.*

Jun. 06 **Theta functions and application to coding theory**, *App. of Computer Algebra*, Varna, Bulgaria.

Apr. 05 **Hyperelliptic curves with reduced automorphism group A_5**, *AMS Meeting, Santa Barbara.*

Jan. 05 **Genus 2 curves that admit a degree 5 map to an elliptic curve**, *Joint AMS Meeting, Atlanta.*

Dec. 04 **Genus 2 curves with (5, 5) split Jacobian**, *Institute for Exp. Math., Essen, Germany.*

Jul. 04 **Field of moduli of curves, a computational approach**, *Workshop Computational Arithmetic Geometry, PIMS Simon Fraiser University..*

Oct. 03 **Genus 2 curves with degree 5 elliptic subcovers**, *AMS Meeting, Chapel Hill.*

Aug. 03 **Determining the automorphism group of algebraic curves**, *ISSAC 03, Drexler University.*

Jul. 03 **Computational aspects of hyperelliptic curves**, *ACA 03, Raleigh, NC.*

Jun. 03 **The monodromy group of a generic curve covering $\mathbb{P}^1$**, *AMS and RSME Meeting, Seville.*

Jun. 03 **Computational aspects of hyperelliptic curves**, *University of Cantabria, Santander, Spain.*

Oct. 03 **Loci of algebraic curves with prescribed group action**, *Algebraic Curves and Cryptography*, University of Florida, Gainesville.

Jan. 03 **Hyperelliptic curves with non-hyperelliptic involutions**, *AMS Joint Meeting, Baltimore.*

Sep. 02 **Hyperelliptic curves with extra automorphisms**, *Galois Theory Conference, John Thompson's 70th birthday, Gainesville, FL.*

Jul. 02 **Genus 2 curves with (3,3)-split Jacobian and large automorphism group**, *ANTS V, International Symposium in Algorithmic Number Theory, Sydney, Australia.*

Nov. 01 **Elliptic subfields of genus 2 fields**, *Groups and Covering Spaces in Algebraic Geometry, AMS Meeting*, UC-Irvine, Irvine, CA.

Sep. 01 **The automorphism group of a Riemann surface**, *Math. Colloquium, Gainesville, Florida.*

Jun. 01 **Elliptic subfields and automorphisms of genus 2 curves**, *University of Erlangen, Germany.*

May 01 **Locus of genus 2 fields with degree 2 or 3 elliptic subfields**, *Institute for Exp. Math.*, Essen.

May 01 **Computational Aspects of Genus 2 Curves**, *Number Theory Conference 2001*, University of Illinois, Urbana-Champaign.

Dec. 00 **Genus 2 curves covering elliptic curves**, *Workshop on Arithmetic Geometry*, Semester on arithmetic geometry, MSRI, Berkeley, CA.

June 00 **Modular curves and Hurwitz spaces**, *Conference on Topological Groups, TU-München, Germany.*

Mar. 00 **Curves of genus two with (n,n)-decomposable Jacobians**, *AG Gruppentheorie*, University of Erlangen, Erlangen, Germany.

May 99 **Explicit equation of certain Hurwitz spaces**, *University of Heidelberg, Germany.*

Mar. 98 **Rigid tuples and monodromy groups**, *Conference on ABC-conjecture*, Tucson, Arizona.

Ph.D. students

current **Jurgen Mezinaj**, Oakland University.
Topic: Machine Learning and invariant theory

2016 **L. Beshaj**, Oakland University.
Thesis: Integral binary forms with minimal height
Position: Associate Professor, Army Cyber Institute, West Point Military Academy

2009 **R. Sanjeeva**, Oakland University.
Thesis: Automorphism Groups of Cyclic Algebraic Curves
Position: Chair, Department of Mathematics, University of Sri Jayewardenepura, Sri Lanka

2008 **G. Wijesiri**, Oakland University.
Thesis: Theta Functions of Algebraic Curves with Automorphisms
Position: Tenured, University of Kelania, Sri Lanka

References

upon request