Tony Shaska Sr.

Department of Mathematics and Statistics
Oakland University
Rochester, MI 48309
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, arithmetic geometry, moduli spaces, weighted projective spaces.

Cybersecurity and Data Protection
Isogeny based cryptography, (ECC), (HCC), Post-Quantum Cryptography (PQC)

Machine Learning and Artificial Intelligence
Mathematics and Artificial Intelligence, Neurosymbolic AI, Equivariant Neural Networks, AI assisted proofs

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**, *University of Michigan - Dearborn (Highest Distinction)*
Overall GPA: 3.95/4.0, **Major GPA:** 4.0/4.0
Major: Mathematics; **Minors:** Computer Science, Statistics

Experience

Jan. 07-current **Founding Editor and Editor in Chief**, *Albanian Journal of Mathematics*

Aug. 07-current **Associate Professor**, *Department of Mathematics and Statistics, Oakland University, MI*

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

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

Jan.08 -Dec.10 **Rector of the University of Vlora**, *University of Vlora*, Albania

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*

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

Aug.96-May.01 **Graduate Teaching Assistant**, *Department of Mathematics*, University of Florida, Gainesville, FL

Jan.95-Aug.96 **Programer/Consultant**, *Computer Business Solutions Inc., Farmington Hills, MI*

Grants

2024 **Nato Science for Piece and Security**, *Quantum-resistant cryptography (QsafeCrypt)*, (pending)

2023-24 **Nato Science for Piece and Security**, *Isogeny based post-quantum cryptography*, Einstein Institute of Mathematics, #*G*6218, Jerusalem, Israel, August 2024

2014 **Nato Advanced Study Institute**, *Hyperelliptic Curve Cryptography*, ISEG. EAP.ASI 984724, Ohrid, North Macedonia

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

2007-10 **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*

Computer Skills

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

Long term visits

- Fall 2023 **Department of Mathematics, University of Michigan**, *Ann Arbor, MI*, sabbatical
- Winter 2015 **Department of Mathematics, Princeton University**, *Princeton, NJ*, sabbatical
- Summer 2014 **Department of Mathematics, University of Pristina**, *Pristina*, Kosovo
- Nov. 2010 **Mathematical Sciences Research Institute**, *Berkeley, CA.*
- Oct. 2009 **Universidad de Cantabria-Santander**, *Spain*
- Summer 07 **Visiting Professor**, *Maria Curie-Sklodowska University*, Lublin, Poland
- Sep. 2006 **Institute of Mathematics and Applications (IMA)**, *University of Minnesota*
- Summer 2006 **Institut für Experimentelle Mathematik**, *Essen*, Germany
- Aug. 2005 **Institute of Mathematics and Applications (IMA)**, *Quantum Computation*, Minnesota
- Dec. 2004 **Institut für Experimentelle Mathematik**, *Essen*, Germany
- June 03 **Universidad de Cantabria-Santander**, *Santander*, Spain
- July 2003 **Institut für Experimentelle Mathematik**, *Essen*, Germany
- Jul. 2002 **University of Sydney**, *Sydney*, Australia
- Jun. 2001 **Universität Erlangen-Nürnberg**, *Erlangen*, Germany
- Summer 2001 **Institut für Experimentelle Mathematik**, *Essen*, Germany
- Dec. 2000 **Mathematical Sciences Research Institute**, *Arithmetic Geometry*
- Jan.-Aug. 2000 **Universität Erlangen-Nürnberg**, *DFG Fellowship*, Germany
- Fall 1999 **MSRI**, *Berkeley, CA*, Galois Groups and Fundamental Groups
- June 1999 **Institute for Advanced Study/Park City Institute**, *Arithmetic Geometry*, Park City, Utah
- Summer 1998 **IWR**, *University of Heidelberg*, Heidelberg, Germany

Editorial

- 2025 **Isogeny based post-quantum cryptography**, *NATO Science for Peace and Security Series - D: Information and Communication Security*, Shaska/Zemel, (to appear)
- 2025 **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**, *Contemporary Mathematics*, 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

Conferences Organized

May 24 **Isogeny based post-quantum cryptography**, *Einstein Institute of Mathematics, The Hebrew University of Jerusalem*

July 24 Galois Theory and Arithmetic, European Congress of Mathematics, Seville, July 15-19, 2024.

April 24 Automorphisms of Riemann surfaces and related topics, AMS Meeting Univ. of Wisconsin-Milwaukee

April 24 Artificial Intelligence in Mathematics, AMS Meeting University of Wisconsin-Milwaukee

July 23 **Algebraic Aspects of Postquantum Cryptography**, *Warsaw, Poland*

Jan. 23 **Excursions in Arithmetic Geometry**, *Special session*, Joint Mathematics Meetings, Boston

June 22 **Recent trends in algebra, geometry, and arithmetic**, Vlora, Albania (with Elira Curri)

Mar. 22 **Curves, Jacobians, and Abelian Varieties**, *AMS Sectional Meeting*, University of Virginia, with A. Obus and P. Srinivasan

Jan. 21 **Algebraic and Arithmetic Geometry**, *Joint Mathematics Meetings*, Washington, DC

Mar. 20 **Cyber defense and cryptography in undergraduate education**, *AMS Meeting*, Charlottesville

Mar. 20 **Curves, Jacobians, and Abelian Varieties**, *AMS Meeting*, Univ. of Virginia, Charlottesville, VA

Dec. 18 **Tirana Winter School in Algebraic Geometry**, *Tiranë*, Albania

Oct. 18 **From hyperelliptic to superelliptic curves**, *Special session, AMS Meeting*, Ann Arbor, MI

Aug. 18 **Algebraic Curves, Integrable Systems, Cryptography**, *Kiev*, (J. Bernatska and V. Enolski)

Mar. 18 **Arithmetic of Algebraic Curves**, *AMS Meeting*, Columbus, OH, with A. Elezi and M. Polak

Jan. 17 **Minimal integral models of algebraic curves**, *AMS Joint Meeting*, Atlanta, GA

Nov. 16 **Varieties, their fibrations and automorphisms in mathematical physics and arithmetic geometry**, *AMS Sectional Meeting*, Raleigh, NC

Jan. 16 **Higher Genus Curves and Fibrations of Higher Genus Curves in Mathematical Physics and Arithmetic Geometry**, *Joint Mathematics Meetings AMS & MAA*, Seattle, WA

Mar. 15 **Arithmetic of Hyperelliptic Curves**, *Special Session*, AMS Meeting, East Lansing, MI

Aug. 14 **Nato Advanced Study Institute**, *Arithmetic of Hyperelliptic Curves*, Ohrid, Macedonia

July 14 **Applications of Computer Algebra**, *Fordham University*, New York, with R. H. Lewis

July 14 **Moduli spaces and arithmetic dynamics**, *Applications of Computer Algebra*, Fordham, NY

July 13 **Arithmetic of algebraic curves**, *Applications of Computer Algebra*, Malaga, Spain

June 12 **Michigan Computational Algebraic Geometry**, *Rochester, MI*

June 12 **East Coast Computer Algebra Day**, *Oakland University*, Rochester, MI, with D. Steffy

Mar. 12 **Computational Algebraic Geometry**, *AMS Sectional Meeting*, Tampa, FL

Jan. 11 **Computational Algebraic and Analytic, Geometry for Low-Dimensional Varieties.**, *AMS Annual Meeting*, New Orleans

June 10 **Applications of Computer Algebra**, *ACA 2010*, Vlora, Albania

Jan. 09 **Computational Algebraic and Analytic, Geometry for Low-Dimensional Varieties**, *AMS Annual Meeting*, Washington DC, with M. Seppala, E. Volchek

May 08 **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 07 **Applications of Computer Algebra**, *ACA 2007*, Rochester, MI

July 07 **Coding theory and cryptography**, *ACA 2006*, Special session, Rochester, MI, with D. Joyner, C. Shor

Jul. 07 **Special session: Computational algebraic geometry**, *ACA 07, Rochester, MI*

Jan. 07 **Computational Algebraic and Analytic, Geometry for Low-Dimensional Varieties**, *AMS Annual Meeting*, New Orleans

June 06 **Coding theory and cryptography**, *Special Session*, ACA 2006, Varna, Bulgaria, with S. Dodunekov

May 05 **Computational aspects of algebraic curves**, *University of Idaho*, Moscow, Idaho

Jan. 05 **Algorithmic Algebraic and Analytic Geometry**, *Special Session*, AMS Annual Meeting, Atlanta

July 04 **Computational aspects of algebraic curves**, Applications of Computer Algebra, Beaumont, TX

July 03 **Computational aspects of algebraic curves**, Applications of Computer Algebra, Raleigh, NC

Sep. 01 **Progress in Galois Theory**, *John Thompson's 70th birthday*, University of Florida, with H. Völklein

Publications

Submitted or in progress

60. T. Shaska; Rational points of weighted hypersurfaces over finite fields
59. T. Shaska; Quantum Gröbner Bases for Weighted Homogeneous Relations in Weighted Projective Spaces
58. E. Badr, E. Shaska, T. Shaska; Rational Functions on the Projective Line from a Computational Viewpoint, *Journal of Symbolic Computation*
57. T. Shaska; Graded Neural Networks (Neus 25)
56. E. Shaska, T. Shaska; Neuro-Symbolic Learning for Galois Groups: A Machine Learning Approach to Polynomial Solvability (Neus25)
55. I. Kostireas, T. Shaska; Reduction of binary forms, Julia invariant, and machine learning, (ISSAC 2025)
54. E. Shaska, T. Shaska; Polynomials, Galois groups, and Neurosymboloic AI, (ISSAC 2025)

Selected papers

53. R. Hidalgo, S. Quispe, T. Shaska; Generalized superelliptic Riemann surfaces, *Transformation Groups*, (being reviewed)
52. E Cotterill, I Darago, C. G Lopez, C Han, T Shaska; Arithmetic inflection of superelliptic curves, *Michigan Math. Journal*, 2025, (to appear)
51. E. Shaska, T. Shaska; Machine learning for moduli space of genus two curves and an application to isogeny based cryptography, *J Algebr Comb*, 61, 23 (2025).
50. S. Salami, T. Shaska; Vojta's conjecture on weighted projective varieties, *European J. Math.*, **11**, 12 (2025).
49. S. Salami, T. Shaska; Local and global heights on weighted projective varieties, *Houston J. Math.* vol. 49, No. 3, 603-636 (2023).
48. A. Clingher, A. Malmendier, T. Shaska; On isogenies among certain Abelian varieties, *Michigan Math. Journal*, 71, No. 2, 227-269 (2022).
47. 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).
46. A. Obus, T. Shaska; Superelliptic curves with many automorphisms and CM Jacobians, *Mathematics of Computation*, **90**, (2021), 332, 2951–2975.
45. L. Beshaj, A. Elezi, T. Shaska;Isogenous components of Jacobian surfaces, *Eur. J. Math.*, **6**, (2020), no. 4, 1276–1302.
44. L. Beshaj, J. Gutierrez, T. Shaska; Weighted greatest common divisors and weighted heights, *J. Number Theory*, 213 (2020), 319-346.
43. A. Clingher, A. Malmendier, T. Shaska; Six line configurations and string dualities, *Commun. Math. Phys.*, (2019) 371, 159-196.
42. A. Malmendier, T. Shaska; The Satake sextic in F-theory, Journal of Geometry and Physics vol. 120, (2017), 290-305
41. T. Shaska, C. Shor 2-Weierstrass points of genus 3 hyperelliptic curves with extra automorphisms, Comm. in Algebra 45 (2017), no. 5, 1879 - 1892.
40. T. Shaska; Genus two curves with many elliptic subcovers, Comm. in Algebra 44 (2016), Nr. 10, 4450-4466
39. T. Shaska, C. Shor Theta functions and complete weight enumerators for codes over imaginary quadratic fields, Des. Codes Cryptogr. vol 76, 2015, 217-235
38. T. Shaska, F. Thompson Bielliptic curves of genus 3 in the hyperelliptic moduli, Appl. Algebra Engrg. Comm. Comput. Volume 24, 2013, 387-412
37. T. Shaska; Some remarks on the hyperelliptic moduli of genus 3, Comm. in Algebra 42 (9), 2014, 4110–4130
36. 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
35. 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
34. T. Shaska, V. Ustimenko On the homogeneous algebraic graphs of large girth and their applications, Linear Algebra Appl. 430 (2009), no. 7, 1826–1837

33. 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

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

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; Decomposition of some Jacobian varieties of dimension 3 Artificial Intelligence and Symbolic Computation LNCS vol. 8884, 193-204

14. L. Beshaj, T. Shaska, C. Shor On Jacobians of curves with superelliptic components Contemp. Math. vol. 29, 14, 1–14

13. 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.

12. 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

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

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

Chapter Books, Biographies

4. G. Hiss and T. Shaska; Kay Magaard (1962–2018), Special issue in honor of Kay Magaard, Albanian J. Math. Vol. 12, (2018), no. 1, 33-35.
3. Alfred J. Menezes, Paul C. van Oorschot, David Joyner, Tony Shaska, Douglas R. Shier, Wayne Goddard; Coding Theory,, Chapter to Handbook of Discrete and Combinatorial Mathematics
2. B. Shaska, T. Shaska; Mësimdhënia e matematikës nëpërmjet problemeve klasike, Albanian J. Math., vol. 10, (2016), no. 1, 47-80.
1. T. Shaska; Computational algebraic geometry J. Symbolic Comput. 57 (2013), 1–2.

Selected talks

Oct. 24 **Machine Learning in Mathematical Research**, *Mathematics Colloquium, Utah State Univ.*

Aug. 24 **Machine models for weighted spaces**, *Data, Numbers, and Geometry, Danger 4*, London Institute for Mathematical Sciences

July 24 **Genus 2 curves with (n,n)-split Jacobians and Isogeny Based Cryptography, Advanced Research Workshop on Isogeny based Crryptography, Jerusalem, July 29-31, 2024**

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*

Oct. 06 **Some open problems in computational geometry**, *Math. Colloquium*, University of Michigan-Dearborn

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*, 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*

Sep. 02 **Field of definition and field of moduli of hyperelliptic curves**, *Math. Colloquium, Gainesville, Florida*
Cancelled because of September 11, 2002

Jul. 02 **Genus 2 curves with (3,3)-split Jacobian and large automorphism group**, *ANTS V, 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*

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

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

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

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

Service

Reviewer for MathSciNet (40 articles reviewed)

Reviewer for Zentralblatt MATH

Committees

2010–13 *Committee on Human Rights, American Mathematical Society*

Reviewer for grants

2003-21 Reviewer for NSA, NSF

University and department committees

2015-22 Graduate Committee, Department of Mathematics and Statistics

2013-15 Graduate Council, College of Arts and Sciences, Oakland University

2010-13 Chair, University Research Committee, Oakland University

2013-14 Graduate Committee, Department of Mathematics and Statistics

2012-13 Undergraduate Committee, Department of Mathematics and Statistics

2011-12 Graduate Committee, Department of Mathematics and Statistics

2012-13 Chair of Colloquium Committee, Department of Mathematics and Statistics

2008-09 Graduate Committee, Department of Mathematics and Statistics

2008-09 Undergraduate Committee, Department of Mathematics and Statistics

2006-07 Graduate Committee, Department of Mathematics and Statistics

2005-06 Graduate Committee, Department of Mathematics and Statistics

2005-06 Chair of Colloquium Committee, Department of Mathematics and Statistics

Teaching

CS 121-122:	Introduction to programing I, II
CS 151-152:	Algorithms and data structures I, II
CS 241-242:	Introduction to Cryptography I, II
CS 451-452:	Theory of Computation I, II
CS 481-482:	Modern Cryptography I, II
EE 431-432:	Source coding, Channel coding
MTH 1663:	Math for Information Technology
MTH 2555:	Intro Diff Eq with Matrix Algebra
MTH 2663:	Discrete Mathematics
MTH 4663:	Graph Theory/Combinatorial Math
MTH 4777:	Computer Algebra
MTH 5005:	Special Topics
MTH 5663:	App Mth: Discrete Methods
MTH 5668:	Math Model in Industry: Discrete
MTH 5777:	Computer Algebra
MTH 5881:	Theory of Computation
MTH 6773:	Coding Theory
MTH 1221:	Linear Prog/Elementary Functions
MTH 1554:	Calculus l, II
MTH 2554:	Calculus III: Multivariable Calculus
MTH 2775:	Linear Algebra
MTH 3002:	Intro Advanced Mathematical Thinking
MTH 4662:	Geometric Structures
MTH 4772:	Number Theory w/Cryptography
MTH 4775:	Abstract Algebra l, II
MTH 5661:	Topology l
MTH 5771:	Algebra l, II
MTH 5990:	Directed Reading and Research
MTH 6770:	Algebraic Number Theory
MTH 6771:	Commutative Algebra
MTH 6772:	Algebraic Geometry
MTH 5905:	Mathematics of Machine Learning

Ph.D. students

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

2016 **L. Beshaj**, Oakland University
Position: Associate Professor, Army Cyber Institute, West Point Military Academy

2009 **R. Sanjeeva**, Oakland University
Position: Chair, Department of Mathematics, University of Sri Jayewardenepura, Sri Lanka

2008 **G. Wijesiri**, Oakland University
Position: Tenured, University of Kelania, Sri Lanka

References

Andreas Malmendier, Utah State University, (andreas.malmendier@usu.edu)
Lubjana Beshaj, West Point Military Academy, (lubjana.beshaj@westpoint.edu)
Ilias Kostireas, Wilfried Laurier University, (ikotsire@wlu.ca)