

Tony Shaska;

Department of Mathematics and Statistics
Oakland University
Rochester, MI 48309

Phone: 248-760-7447
E-mail: shaska@oakland.edu
Webpage: www.risat.org/people/shaska/
Others: [ArXiv](#) [Google Scholar](#)



Research areas

Algebraic and Arithmetic Geometry.

Algebraic curves, automorphisms, hyperelliptic and superelliptic curves, Hurwitz spaces and moduli spaces of curves, weighted projective spaces and their heights, minimal models of curves, cryptography, etc.

Education

- Sep.96-Mar.01 **Ph.D. in Mathematics**, *The University of Florida*, Gainesville, FL.
Thesis: Curves of genus two covering elliptic curves
- Jan.92-Dec.94 **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

- 2009-current **Professor of Mathematics**, *Ministry of Education and Sciences*, Albania.
- 2007-current **Founding Editor and Editor in Chief**, *Albanian Journal of Mathematics*.
- Jan.08 -Dec.10 **Rector**, University of Vlora, Vlora, Albania.
- 2008-current **Associate Professor**, *Department of Mathematics and Statistics*, Oakland University, MI.
- Aug.05-Aug.08 **Assistant Professor**, *Department of Mathematics and Statistics*, Oakland University, MI.
- Aug.03-Jun.05 **Assistant Professor**, *Department of Mathematics*, University of Idaho, ID.
- Aug.01-Jun.03 **Visiting Assistant Professor**, *Department of Mathematics*, University of California–Irvine, CA.
- Aug.96-May.01 **Teaching Assistant**, *Department of Mathematics*, University of Florida, FL.

Long term visits

- Winter 15 **Princeton University**, *Sabbatical*, Department of Mathematics, Host: Manjul Bhargava.
- Jun. 13 **Linkoping University**, *Linkoping*, Sweden, Host: Milagros Izquierdo.
- Summer 12 **University of Pristina**, *Pristina*, Kosova, Host: Qëndrim Gashi.
- Oct. 09 **Universidad de Cantabria-Santander**, *Spain*, Host: J. Gutierrez.
- Winter 08 **University of Vlora**, *Sabbatical*, *Department of Mathematics*, Vlora, Albania.
- Jun. 07 **Boston University**, *Department of Mathematics*, Host: Emma Previato.
- Summer 07 **Maria Curie-Sklodowska University**, *Lublin*, Poland, Host: Vasyl Ustimenko.
- Summer 06 **Institut für Experimentelle Mathematik**, *Essen*, Germany, Host: Helmut Voelklein.
- Aug. 05 **Institute of Mathematics and Applications (IMA)**, *Quantum Computation*, Minnesota.
- Summer 03 **Universidad de Cantabria-Santander**, *Spain*, Host: J. Gutierrez.
- Summer 03 **Institut für Experimentelle Mathematik**, *Essen*, Germany, Host: Gerhard Frey.
- Summer 01 **Institut für Experimentelle Mathematik**, *Essen*, Germany, Host: Gerhard Frey.
- Dec. 00 **Mathematical Sciences Research Institute**, *Arithmetic Geometry*.
- Jan.-Aug. 00 **Universität Erlangen-Nürnberg**, *DFG Fellowship*, Germany, Host: Karl Strambach.
- Fall 99 **Mathematical Sciences Research Institute**, *Berkeley*, CA.
- Jun. 99 **Institute for Advanced Study/Park City Institute**, *Arithmetic Geometry*, Park City, Utah.
- Summer 98 **IWR**, *University of Heidelberg*, Heidelberg, Germany, Host: Heinrich Matzat.

Awards and Grants

- 2014 **Nato Advanced Study Institute**, *Hyperelliptic Curve Cryptography*, ISEG. EAP.ASI 984724.
2012 **National Security Agency**, *Conference Grant*, 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*.
01 **Threadgill Dissertation Award**, *Department of Mathematics*, University of Florida, Gainesville, FL.
Dec. 1994 Graduated with Highest Distinction, University of Michigan

Editorial

- 2007-present **Founding Editor and Editor in Chief**, *Albanian Journal of Mathematics*.

Editor for volume proceedings

- 2021 **Abelian varieties and number theory**, *Contemporary Mathematics*, Celebration of Gerhard Frey's 75th birthday, (AMS),, Moshe Jarden, Tony Shaska (Eds.).
2020 **Integrable systems and Algebraic Geometry**, *Volume 1*, Cambridge University Press, ISBN: 9781108773287, Ron Donagi and Tony Shaska (Eds.).
2020 **Integrable systems and Algebraic Geometry**, *Volume II*, Cambridge University Press, ISBN: 9781108773355, Ron Donagi and Tony Shaska (Eds.).
2019 **Algebraic curves and their applications**, *Contemporary Mathematics*, Volume: 724; 19; 344 pp; Softcover MSC: Primary 11; 14; Print ISBN: 978-1-4704-4247-7, L. Beshaj, T. Shaska (Eds.).
2018 **Higher Genus Curves in Mathematical Physics and Arithmetic Geometry**, *Contemporary Mathematics*, (703), 18. vii+222 pp. ISBN: 978-1-4704-2856-3, A. Malmendier, T. Shaska (Eds.).
2015 **Advances on superelliptic curves and their applications**, *NATO Science for Peace and Security Series - D: Information and Communication Security*, Vol 41. 15, L. Beshaj, T. Shaska, E. Zhupa.
2009 **Algebraic Aspects of Digital Communications**, *NATO Science for Peace and Security Series, D: Information and Communication Security*, Vol. 24. 09. viii+285 pp, T. Shaska (Ed).
2007 **Advances in coding theory and cryptology**, *Series: Coding Theory and Cryptography*, Vol. 3, World Scientific Publishing, xii+256 pp, W. C. Huffman, D. Joyner, T. Shaska, V. Ustimenko (Eds).
2005 **Computational aspects of algebraic curves**, *Lecture Notes in Computing Series*, World Scientific, vol. 13, (05), 288pp, ISBN 981-256-459-4, T. Shaska (Ed).
2005 **Progress in Galois Theory**, *Proceedings of J. Thompson's 70-th birthday*, Springer Series: Developments in Mathematics, Vol. 12, 168 pp, H. Völklein, T. Shaska (Eds.).

Editor for special issues of journals

- 2018 **Special issue in memory of Kay Magaard**, *Albanian J. Math.* (2018).
2013 **Computational algebraic geometry and its applications**, *Appl. Algebra Engrg. Comm. Comput. Vol. 24, 1-98, 13.*
2013 **Computational Algebraic Geometry**, *J. Symbolic Comp. Vol. 57, Oct. 13, 1-78.*
2010 **Applications of Computer Algebra**, *Albanian J. Math. Vol 4, No 4, (10).*
2008 **New challenges in digital communications**, *Albanian J. Math., Vol 2, No 3, (08).*
2007 **Computational Algebraic Geometry**, *Albanian J. Math., Vol 1., No 4, (07).*
2007 **Coding theory and cryptography**, *Serdica J. Comput., Vol. 1, No. 2, 07.*

Books

- **From hyperelliptic to superelliptic curves**, (in preparation), 21.

Papers

Journal articles

39. Ethan Cotterill, Ignacio Darago, Cristhian Garay López, Changho Han, Tony Shaska; [Arithmetic inflection of superelliptic curves](#), *Michigan Math.* (submitted)
38. A. Clingher, A. Malmendier, T. Shaska; [Geometry of Prym varieties for special bielliptic curves of genus three and five](#), *Pure and Applied Mathematics Quarterly*, 2022. (to appear)
37. A. Clingher, A. Malmendier, T. Shaska; [On isogenies among certain Abelian varieties](#), *Michigan Math.* 2022, (to appear)
36. A. Obus, T. Shaska; [Superelliptic curves with many automorphisms and CM Jacobians](#), *Math. Comp.*, **90**, (2021), 332, 2951–2975.
35. A. Elezi, T. Shaska; [Reduction of binary forms via the hyperbolic centroid](#), *Lobachevskii J. Math.* **42**, (2021), 1, 84–95.
34. L. Beshaj, A. Elezi, T. Shaska; [Isogenous components of Jacobian surfaces](#), *Eur. J. Math.* **6**, (2020), no. 4, 1276–1302.
33. L. Beshaj, J. Gutierrez, T. Shaska; [Weighted greatest common divisors and weighted heights](#), *J. Number Theory*, 213 (2020), 319–346.
32. A. Clingher, A. Malmendier, T. Shaska; [Six line configurations and string dualities](#), *Commun. Math. Phys.*, (2019) 371: 159–196.
31. A. Malmendier, T. Shaska; [From hyperelliptic to superelliptic curves](#), *Albanian J. Math.*, **13**, (2019), No. 1. pg. 107–200.
30. Shuichi Otake, Tony Shaska; [Some remarks on the non-real roots of polynomials](#), *Cubo*, (2019), 67–93. 18, no. 1, 33–35.
29. 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.
28. 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
27. A. Malmendier, T. Shaska; [The Satake sextic in \$F\$ -theory](#), *Journal of Geometry and Physics* vol. 120, (2017), 290–305
26. T. Shaska, C. Shor [2-Weierstrass points of genus 3 hyperelliptic curves with extra automorphisms](#), *Comm. in Algebra* 45 (2017), no. 5, 1879 - 1892.
25. T. Shaska; [Genus two curves with many elliptic subcovers](#), *Comm. in Algebra* 44 (2016), Nr. 10, 4450–4466
24. T. Shaska, C. Shor [Theta functions and complete weight enumerators for codes over imaginary quadratic fields](#), *Des. Codes Cryptogr.* vol 76, 2015, 217–235
23. T. Shaska, F. Thompson [Bielliptic curves of genus 3 in the hyperelliptic moduli](#), *Appl. Algebra Engrg. Comm. Comput.* Volume 24, 2013, 387–412
22. T. Shaska; [Some remarks on the hyperelliptic moduli of genus 3](#), *Communications in Algebra* 42 (9), 2014, 4110–4130
21. A. Elezi, T. Shaska; [Quantum codes from superelliptic curves](#), *Albanian J. Math.* Vol. 5. Nr. 4, 2011, pg. 175–191
20. L. Beshaj, V. Hoxhaj, T. Shaska; [On superelliptic curves of level \$n\$ and their quotients](#), *Albanian J. Math.*, Vol. 5. Nr. 3, pg. 115–138, 2011
19. 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
18. 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
17. T. Shaska, V. Ustimenko [On the homogeneous algebraic graphs of large girth and their applications](#), *Linear Algebra Appl.* 430 (2009), no. 7, 1826–1837
16. T. Shaska, V. Ustimenko [On some applications of graphs to cryptography and turbocoding](#), *Albanian J. Math.*, Vol 2, Nr. 3, 2008, 249 – 255.
15. 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
14. T. Shaska; [Quantum codes from algebraic curves with automorphisms](#), *Condensed Matter Physics* Vol. 11, 2008, No 2 (54), 383–396.

13. T. Shaska, R. Sanjeeva [Determining equations of families of cyclic curves](#), Albanian J. Math. Vol 2, Nr. 3, 2008, 199-213
12. 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
11. 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
10. E. Previato, T. Shaska, G. Wijesiri [Thetanulls of cyclic curves of small genus](#), Albanian J. Math. vol. 1, Nr. 4, 2007, 253-270
9. T. Shaska; [Some open problems in computational algebraic geometry](#), Albanian J. Math vol I, Nr. 3, 07, 297-319
8. T. Shaska, Q. Wang; [Automorphism groups of AG-codes based on \$C_{ab}\$ curves](#), Serdica J. Computing Vol.1, Nr. 1, 2007, 193-206
7. T. Shaska; [Hyperelliptic curves with reduced automorphism group \$A_5\$](#) , Appl. Algebra Engrg. Comm. Comput. vol. 18, Nr. 1-2, 2007, pg. 3-20
6. T. Shaska; [Subvarieties of the hyperelliptic moduli determined by group actions](#), Serdica Math. Journal No. 4, (2006), 355-374
5. J. Gutierrez, T. Shaska; [Hyperelliptic curves with extra involutions](#), LMS J. of Comp. Math. 8, (2005), 102-115.
4. T. Shaska; [Some special families of hyperelliptic curves](#), J. Algebra Appl. 3 (2004), no. 1, 75-89
3. T. Shaska; [Genus 2 fields with degree 3 elliptic subfields](#), Forum Math. 16 (2004), no. 2, 263-280
2. K. Magaard, T. Shaska, S. Shpectorov, H. Völklein; [The locus of curves with prescribed automorphism group](#), Communications in arithmetic fundamental groups (Kyoto, 99/01). *Sūrikaisekikenkyūsho Kōkyūroku* No. 1267 (2002), 112-141
1. T. Shaska; [Curves of Genus 2 with \$\(n, n\)\$ -decomposable Jacobians](#), Jour. Symb. Comp. vol.31, No.5, pg. 603-617, 2001

Conference Proceedings

26. T. Shaska; [Reduction of superelliptic Riemann surfaces](#) Contemporary Math., (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 quadrimomials](#) 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 and 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 and 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 and 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

- Jan. 21 [Algebraic and Arithmetic Geometry](#), Joint Mathematics Meetings, Washington, DC, (with Marc Hindry)
- Mar. 20 [Cyber defense and cryptography in undergraduate education](#), AMS Sectional Meeting, University of Virginia, Charlottesville, VA (cancelled)
- Mar. 20 [Curves, Jacobians, and Abelian Varieties](#), University of Virginia, Charlottesville, VA. with A. Obus and P. Srinivasan (cancelled)
- Dec. 18 [Tirana Winter School in Algebraic Geometry](#), Tiranë, Albania, Dec. 28-29, 18.
- Oct. 18 [From hyperelliptic to superelliptic curves](#), Spring Central Sectional Meetings in University of Michigan, Meeting 1143. (with Yuri Zarhin and Nicola Tarasca)
- Aug. 18 [Algebraic Curves, Integrable Systems, Cryptography](#) (with Julia Bernatska and Victor Enolski), Kiev, Ukraine, Aug. 24-25, 18
- Mar. 18 [Arithmetic of Algebraic Curves](#), Spring Central Sectional Meetings in Ohio State University, Meeting 1136. (with A. Elezi and M. Polak)
- Jan, 17 [Minimal integral models of algebraic curves](#), AMS Joint Meeting, Jan. 17, Atlanta, GA.
- Nov. 16 [Varieties, their fibrations and automorphisms in mathematical physics and arithmetic geometry](#), AMS Sectional Meeting, Nov. 16, Raleigh, NC.
- Jan. 16 [Special Session on Higher Genus Curves and Fibrations of Higher Genus Curves in Mathematical Physics and Arithmetic Geometry](#), Joint Mathematics Meetings AMS & MAA, Washington State Convention Center, Seattle, WA, Jan. 6-9, 16
- Mar. 15 Special Session: Arithmetic of Hyperelliptic Curves, Michigan State University, East Lansing, MI.
- Aug. 14 [Nato Advanced Study Institute](#), Arithmetic of Hyperelliptic Curves, Ohrid, Macedonia.
T. Shaska, E. Zhupa
- Jul. 14 [Applications of Computer Algebra \(ACA 14\)](#), Fordham University, New York. R. H. Lewis, T. Shaska;
14 Co-organizer: Moduli spaces and arithmetic dynamics, Special Session, ACA 14, Fordham, New York, Jul. 9-12, 14

- Jul. 13 [Arithmetic of algebraic curves](#), ACA 13, Malaga, Spain. (with J. M. Couveignes, N. Pagani)
- Jun. 12 MCAG 12: [Michigan Computational Algebraic Geometry 12](#), Oakland University, Rochester, MI.
Tony Shaska, Dan Erman, Charles Wampler
- Jun. 12 ECCAD 12: East Coast Computer Algebra Day, Oakland University, Rochester, MI.
T. Shaska, D. Steffy
- Mar. 12 Special Session: Computational Algebraic Geometry, AMS Sectional Meeting, Tampa, FL.
A. Elezi, T. Shaska;
- Jan. 11 Computational Algebraic and Analytic, Geometry for Low-Dimensional Varieties. AMS Annual Meeting, New Orleans (with M. Seppala, E. Volchek)
- Jun. 10 General Chair: Applications of Computer Algebra, ACA 10, Jun. 24-27, 10, University of Vlora, supported by Ministry of Science and Education, Albania.
T. Shaska, E. Ruci, E. Zhupa, J. Calmet, A. Akritas, M. Wester
- Jan. 09 Special Session: 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;
- Jul. 07 Applications of Computer Algebra, ACA 07, Oakland University, Rochester, MI.
- Jul. 07 Special session: [Coding theory and cryptography](#), ACA 07, Rochester, MI.
D. Joyner, T. Shaska, C. Shor
- Jul. 07 Special session: Computational algebraic geometry, ACA 07, Rochester, MI.
A. Elezi, T. Shaska;
- Jan. 07 Special Session: Computational Algebraic and Analytic, Geometry for Low-Dimensional Varieties. AMS Annual Meeting, New Orleans
M. Seppala, E. Volchek, T. Shaska;
- Jun. 06 Special Session: Coding theory and cryptography, ACA 06, Varna, Bulgaria.
S. Dodunekov, T. Shaska;
- May 05 Computational aspects of algebraic curves, University of Idaho, Moscow, Idaho, 05.
- Jan. 05 *Special Session: Algorithmic Algebraic and Analytic Geometry*, AMS Annual Meeting, Atlanta, GA.
M. Seppala, E. Volchek, T. Shaska;
- Jul. 04 Special session: *Computational aspects of algebraic curves*, ACA 04, Beaumont, TX.
- Jul. 03 Special session: [Computational aspects of algebraic curves](#), ACA 03, NC State, Raleigh, NC.
- Sep. 01 Progress in Galois Theory, John Thompson's 70th birthday
H. Völklein, T. Shaska;

Selected talks

- May 20 [The arithmetic of weighted moduli spaces](#), NATO Advanced Study Institute: Recent trends in cryptology and cyber security, Kyiv, Ukraine
- Mar. 20 [Computation on moduli spaces: an introduction to weighted moduli heights](#), AMS Section Meeting, Special Session on Moduli of Curves, Hilbert Schemes, and Tropical Geometry, Tufts University, Medford, MA.
- Mar. 20 [The addition on Jacobian varieties from a geometric viewpoint](#), AMS Section Meeting, Special Session on Automorphisms of Riemann Surfaces, Subgroups of Mapping Class Groups and Related Topics, Tufts University, MA.
- Mar. 20 [Educating the good citizen: an algebraic viewpoint](#), AMS Section Meeting, Special Session on Cyber defense and cryptography in undergraduate education, University of Virginia, Charlottesville, VA,
- Mar. 20 [Weighted greatest common divisors and weighted heights](#), AMS Section Meeting, Special Session on Curves, Jacobians, and Abelian Varieties, University of Virginia, Charlottesville, VA.

- Dec. 19 [Heights on weighted projective varieties](#), Department of Mathematics Colloquium, University of Sarajevo, Sarajevo, Bosnia and Herzegovina.
- Oct. 19 [Addition on Jacobian varieties from a geometric viewpoint](#), National University of Greece, Athens, Greece.
- Apr. 19 [Abelian varieties with complex multiplication](#), Explicit Methods for Abelian and Calabi-Yau varieties, Utah State University, Logan, UT.
- Apr. 19 [Isogenies of 2-dimensional Jacobians](#), Mathematical Cryptology, Spring Eastern Sectional Meeting University of Connecticut Hartford, Hartford, CT
- Mar. 19 [Curves, automorphisms, and their Jacobians](#), Algebra seminar, College of Charleston, Charleston, SC.
- Feb. 19 [Superelliptic curves with complex multiplication](#), Special session: Automorphisms of curves, Santander, Spain.
- Nov. 18 [Heights on weighted projective spaces](#), Algebra Seminar, Wayne State University, Detroit, MI.
- Oct. 18 [Heights on weighted projective spaces](#), AMS Special Session: From hyperelliptic to superelliptic curves, 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, Utah
- Apr. 18 [Riemann surfaces with extra automorphisms and endomorphism rings of their Jacobians](#), Special Session on Automorphisms of Riemann Surfaces and Related Topics, AMS Sectional Meeting in Portland, OR. Apr. 14-15, 18.
- Mar. 18 [Isogenies of Abelian varieties](#), Algebraic curves and their applications, AMS Sectional Meeting in Columbus, OH.
- Sep. 17 [From hyperelliptic to superelliptic curves](#), Algebraic curves and their applications, AMS Sectional Meeting in Orlando, FL. Sep. 22-23, 17.
- Apr. 17 [From hyperelliptic to superelliptic curves](#), Department of Mathematics, US Naval Academy, Apr. 22, 17.
- Jan. 17 [A pair of universal curves of genus 2](#), AMS Joint Meeting in Atlanta, GA. Jan., 4-7, 17.
- Oct. 15 [Theta functions and symmetric weight enumerators for codes over imaginary quadratic fields](#), AMS Special Session on Coding Theory and Its Applications, Chicago, Oct. 3-4, 15
- Oct. 15 [Julia quadratic of superelliptic Riemann surfaces](#), AMS Special Session on Riemann surfaces and their automorphisms, Chicago, Oct. 3-4, 15
- Jun. 15 [Integral minimal models for binary forms](#), Mathematics Colloquium, University of Florida, Gainesville.
- Mar. 15 [Binary forms of minimal height](#), AMS Sectional Meeting, East Lansing
- Jul. 14 [Heights on algebraic curves](#), NATO ASI, Ohrid, 15
- Jul. 14 [Minimal models for curves over their minimal field of definition](#), ACA 14, New York.
- Jul. 14 [Genus 3 hyperelliptic curves with \(2, 4, 4\) split Jacobians](#), ACA 14, New York.
- Mar. 14 [Minimal equations of curves over their minimal field of definition](#), Southeastern Spring Sectional Meeting University of Tennessee, Knoxville, Meeting #1097
- 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](#), AMS Special Session on on Computational Advances on Special Functions and Tropical Geometry, Iowa State University
- May 13 [Stratifications on moduli spaces of curves and superelliptic loci](#), MCAG 13, Western Michigan University
- Mar. 13 [Genus 3 hyperelliptic curves with split Jacobians and many rational points](#), Mathematics Colloquium, Georgia Southern University
- 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](#), Mathematics Colloquium, Duquesne University
- Jun. 12 [A historical view of theta functions \(plenary talk\)](#), Conference on Applications of Algebra, Yildiz University, Istanbul, Turkey

- Mar. 12 [Thetanulls of algebraic curves and some applications](#), AMS Special session on Computational Algebraic Geometry, Tampa, Florida
- Jan 12 [Interesting families of algebraic curves](#), Joint AMS Meeting, Special Session on Mathematics of Computation, Boston
- Jan. 12 [Half-integer theta-nulls of superelliptic curves](#), AMS Sectional Meeting: Special Session on Computational and Algorithmic Algebraic Geometry, Salt Lake City
- Oct. 11 [Theta Functions of algebraic curves](#), Special Session on theta functions, SIAM National Conference, Raleigh
- 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](#), Workshop on Mathematical Cryptology, University of Cantabria, Spain
- Mar. 08 [Theta functions in coding theory](#), Mathematics Colloquium, University of Delaware
- Oct. 07 [Genus 2 curves covering elliptic curves](#), Mathematics Colloquium, Simon Fraser University, Vancouver
- Oct. 07 [Equations of curves with automorphisms](#), AMS Sectional Meeting, Special Session on Numerical and Symbolic Techniques in Algebraic Geometry and Its Applications, DePaul University
- Sep. 07 [Remarks on some old problems of algebraic geometry](#), Mathematics Colloquium, Michigan Tech.
- May 07 [A historical view of theta functions](#), Mathematics Colloquium, Lublin, Poland
- Aug. 06 [Codes over rings of size four, lattices, and their theta functions](#), Mathematics Colloquium, Lublin, Poland
- Oct. 06 [Some open problems in computational geometry](#), Mathematics Colloquium, University of Michigan-Dearborn
- May 06 [Theta functions and automorphism groups of curves](#), Galoistheorie Kolloquium, Institut für Experimentelle Mathematik (IEM), Essen, Germany
- Jun. 06 [Theta functions and application to coding theory](#), (ACA 06), Varna, Bulgaria
- Apr. 05 [Hyperelliptic curves with reduced automorphism group \$A_5\$](#) , AMS Western section, 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 Experimental Mathematics, Essen, Germany
- Jul.. 04 [Field of moduli of curves, a computational approach](#), Workshop Computational Arithmetic Geometry, PIMS Simon Fraser University, Vancouver
- Oct. 03 [Genus 2 curves with degree 5 elliptic subcovers](#), 991-14-21 AMS, Southeastern Section Meeting, Chapel Hill
- Aug. 03 [Determining the automorphism group of algebraic curves](#), ISSAC 03, Drexler University, Philadelphia
- Jul. 03 [Computational aspects of hyperelliptic curves](#), ACA 03, Raleigh, NC
- Jun. 03 [The monodromy group of a generic curve covering \$\mathbb{P}^1\$](#) , Joint International Meeting of AMS and RSME, Seville, Spain
- Jun. 03 [Computational aspects of hyperelliptic curves](#), University of Cantabria, Santander, Spain
- Oct. 03 [Loci of hyperelliptic curves with prescribed group action](#), Computational Aspects of Algebraic Curves, and Cryptography, Gainesville
- Jan. 03 [Hyperelliptic curves with non-hyperelliptic involutions](#) 983-14-115 AMS, JMN, Baltimore
- Sep. 02 [Hyperelliptic curves with extra automorphisms](#), Galois Theory Conference, John Thompson's 70th birthday, University of Florida, Gainesville
- Sep. 02 [Field of definition and field of moduli of hyperelliptic curves](#), University of Florida Colloquium, Gainesville, Florida
- Dec. 02 [Computational aspects of algebraic geometry](#), Algebra seminar, UC Irvine, Irvine, CA
- 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 [Automorphisms and elliptic subfields of genus 2 fields \(with H. Völklein\)](#), 972-14-47 AMS, Southwestern Conference, Groups and Covering Spaces in Algebraic Geometry, Irvine, CA

- Sep. 01 [The automorphism group of a Riemann surface](#), University of Florida Colloquium, Gainesville, Florida
- Jun. 01 [Elliptic subfields and automorphisms of genus 2 curves](#), University of Erlangen, Germany
- May 01 [Computing the locus of genus 2 fields with degree 2 or 3 elliptic subfields](#), Institute for Experimental Mathematics, Essen, Germany
- May 01 [Some Computational Aspects of Genus 2 Curves](#), Number Theory Conference, University of Illinois, Urbana-Champaign, IL
- Dec. 00 [Genus 2 curves covering elliptic curves](#), Workshop on Arithmetic Geometry, MSRI, Berkeley, CA
- Jun. 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, Erlangen, Germany
- May 99 [Explicit equation of certain Hurwitz spaces](#), University of Heidelberg, Germany

Ph.D. students

- 2011-16 **L. Beshaj**, *Ph.D. Mathematics*, Oakland University.
 Thesis: Integral binary forms with minimal height
 Position: Assistant Professor, Army Cyber Institute, West Point Military Academy
- 2005-09 **R. Sanjeeva**, *Ph.D. Mathematics*, Oakland University.
 Thesis: Automorphism Groups of Cyclic Algebraic Curves
 Position: Chair, Department of Mathematics, University of Sri Jayewardenepura, Sri Lanka
- 2005-08 **G. Wijesiri**, *Ph.D. Mathematics*, Oakland University.
 Thesis: Theta Functions of Algebraic Curves with Automorphisms
 Position: Tenured, University of Kelania, Sri Lanka

Teaching

Oakland University

- MTH 1554: Calculus I
- MTH 1555: Calculus II
- MTH 4554: Calculus III
- MTH 2663: Discrete Mathematics
- MTH 2775: Linear Algebra
- MTH 3002: Logic and Proofs
- MTH 4662: Geometry
- MTH 4775-4776: Algebra I, II
- MTH 5771-5772: Graduate Algebra I-II
- MTH 5777: Computational Algebra
- MTH 6770: Commutative Algebra
- MTH 6771: Algebraic Number Theory
- MTH 6772: Algebraic Geometry
- APM 6773: Coding Theory
- APM 5881: Theory of Computation
- APM 5005: Algebraic geometry methods in engineering
- APM 5005: Topics in Cryptology
- APM 5663: Graph Theory and Combinatorial Math

University of Idaho

- Linear Algebra, Introduction to Cryptography Abstract Algebra, Galois Theory, Group Theory
 Computer Security and Cryptography

UC Irvine

- Calculus I, II, III
 Infinite Series and Complex Numbers,

Elementary Linear Algebra, Linear Algebra I, II.

University of Florida

Precalculus, Calculus I, II, Linear Algebra

Service

Reviewer for MathSciNet (40 articles reviewed)

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

2003–21 Reviewer for NSA

2005–21 Reviewer for NSF

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

References

upon request