

Tony Shaska

Department of Mathematics and Statistics
Oakland University
Rochester, MI 48309

Phone: 248-370-3436 (office)
E-mail: shaska@oakland.edu
Webpage: www.oakland.edu/~shaska
Others: [ArXiv](#) [Google Scholar](#)



Research areas

Arithmetic and algebraic geometry, computational algebra, symbolic computation.

hyperelliptic and superelliptic curves, moduli spaces, minimal models of curves, binary forms, decomposable Jacobians, 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

Work Experience

Aug. 08 – **Associate Professor**, *Department of Mathematics and Statistics*, Oakland University, MI.

May. 09 – **Professor of Mathematics**, *Ministry of Education and Sciences*, Albania.

Jan.08 -Jan.11 **Rector**, *University of Vlora*, Vlora, Albania.

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.

Long term visits

Winter 15 **Princeton University**, *Sabbatical*, Department of Mathematics, Host: Manjul Bhargava.

June 13 **Linköping University**, *Linköping*, 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.

June 07 **Boston University**, *Department of Mathematics*, Host: Emma Previato.

Summer 07 **Maria Curie-Sklodowska University**, *Lublin*, Poland, Host: Vasył Ustimenko.

Summer 06 **Institut für Experimentelle Mathematik**, *Essen*, Germany, Host: Helmut Voelklein.

August 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.

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

Summer 98 **IWR**, *University of Heidelberg*, Heidelberg, Germany, Host: Heinrich Matzat.

Editorial

Journals

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

Editor for volume proceedings

- 2020 **Abelian varieties and number theory**, *Contemporary Mathematics*, (in preparation), Celebration of Gerhard Frey's 75th birthday.
Moshe Jarden, Tony Shaska (Eds.)
- 2020 **Integrable systems and Algebraic Geometry**, *Volume 1*, Cambridge University Press, ISBN: 9781108773287, A celebration of Emma Previato's 65th birthday.
Ron Donagi and Tony Shaska (Eds.)
- 2020 **Integrable systems and Algebraic Geometry**, *Volume II*, Cambridge University Press, ISBN: 9781108773355, A celebration of Emma Previato's 65th birthday.
Ron Donagi and Tony Shaska (Eds.)
- 2019 **Algebraic curves and their applications**, *Contemporary Mathematics*, Volume: 724; 2019; 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), American Mathematical Society, Providence, RI, 2018. 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. IOS Press, Amsterdam, 2015, viii+388 pp, ISBN: 978-1-61499-519-7, .
L. Beshaj, T. Shaska, E. Zhupa (Eds.)
- 2009 **Algebraic Aspects of Digital Communications**, *NATO Science for Peace and Security Series, D: Information and Communication Security*, Vol. 24. IOS Press, Amsterdam, 2009. viii+285 pp, ISBN: 978-1-60750-019-3, T. Shaska (Ed).
- 2007 **Advances in coding theory and cryptology** , *Series: Coding Theory and Cryptography*, Vol. 3, World Scientific Publishing, xii+256 pp, ISBN: 978-981-270-701-7; 981-270-701-8, .
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, (2005), 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, ISBN: 0-387-23533-7, .
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, 2013.
- 2013 **Computational Algebraic Geometry**.
J. Symbolic Comp. Vol. 57, October 2013, 1-78
- 2010 **Applications of Computer Algebra**.
Albanian J. Math. Vol 4, No 4, (2010)
- 2008 **New challenges in digital communications**.
Albanian J. Math., Vol 2, No 3, (2008)
- 2007 **Computational Algebraic Geometry**.
Albanian J. Math., Vol 1., No 4, (2007).
- 2007 **Coding theory and cryptography**.
Serdica J. Comput., Vol. I, No. 2, 2007

Books

In progress

- **From hyperelliptic to superelliptic curves**, (in preparation), 2019.

Others

- **Kalkulus dhe Gjeometri Analitike**, ISBN: 978-1-60985-025-8, 2019 .
- **Algjebra**, AulonnaPress, Tiranë, 2014, xvi+1024pp. ISBN: 978-1-60985-013-5.
- **Algjebra Lineare**, Libri Shkollor, Tiranë, 2009..
- **Kurbat Algjebrike**, ISBN: 978-1-60985-016-6, 2018 .

Papers

In progress

- **T. Shaska**, *Stability of binary forms*.
- **T. Shaska**, *Weighted generalized greatest common divisors and Vojta's conjecture for blowups*..
- **T. Shaska, D. Tabaku**, *Cartier and Weil divisors on weighted projective spaces*.
- **A. Obus, T. Shaska**, *Superelliptic Jacobians with complex multiplication*.

Submitted

- **J. Gutierrez, T. Shaska**, *Equations for superelliptic curves with minimal invariants*.
- **Y. Kapeliovich, T. Shaska**, *The addition on Jacobian varieties from a geometric viewpoint*.
- **L. Beshaj, J. Gutierrez, T. Shaska**, *Weighted greatest common divisors and weighted heights* .
- **A. Clinger, A. Malmendier, T. Shaska**, *On isogenies among certain Abelian varieties*.
- **R. Hidalgo, S. Quispe, T. Shaska**, *On generalized superelliptic Riemann surfaces*.

Journal articles

- **L. Beshaj, A. Elezi and T. Shaska**, *Isogenous components of Jacobian surfaces*, European Journal of Mathematics, 2019.
DOI 10.1007/s40879-019-00375-y
- **A. Clinger, A. Malmendier, T. Shaska**, *Six line configurations and string dualities*, Commun. Math. Phys. (2019) 371: 159–196..
<https://doi.org/10.1007/s00220-019-03372-0>
- **A. Malmendier, T. Shaska**, *From hyperelliptic to superelliptic curves*, Albanian J. Math., Vol. 13. (2019), No. 1. pg. 107-200..
<http://albanian-j-math.com/archives/2019-03.pdf>
- **Shuichi Otake and Tony Shaska**, *Some remarks on the non-real roots of polynomials* , Cubo, (2019), 67-93., 2018, no. 1, 33-35..
- **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..
- **A. Malmendier and 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.
<https://www.emis.de/journals/SIGMA/2017/089/>
- **A. Malmendier and T. Shaska**, *The Satake sextic in F -theory*, Journal of Geometry and Physics, vol. 120, (2017), 290-305.
<https://www.sciencedirect.com/science/article/pii/S0393044017301663>
- **T. Shaska and C. Shor**, *2-Weierstrass points of genus 3 hyperelliptic curves with extra automorphisms*, Comm. in Algebra, 45 (2017), no. 5, 1879 - 1892..
<https://www.tandfonline.com/doi/abs/10.1080/00927872.2016.1226861?journalCode=lagb20>
- **T. Shaska**, *Genus two curves with many elliptic subcovers*, Comm. in Algebra, 44 (2016), Nr. 10, 4450-4466.
<https://www.tandfonline.com/doi/abs/10.1080/00927872.2015.1027365?journalCode=lagb20>

- **T. Shaska and C. Shor**, *Theta functions and complete weight enumerators for codes over imaginary quadratic fields*, Des. Codes Cryptogr., vol 76, 2015, 217-235.
- **T. Shaska and F. Thompson**, *Bielliptic curves of genus 3 in the hyperelliptic moduli*, Appl. Algebra Engrg. Comm. Comput., Volume 24, 2013, 387-412.
- **T. Shaska**, *Some remarks on the hyperelliptic moduli of genus 3*, Communications in Algebra, 42(9), 2014, 4110–4130.
- **A. Elezi and T. Shaska**, *Quantum codes from superelliptic curves*, Albanian J. Math., Vol. 5. Nr. 4, 2011, pg. 175–191.
- **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.
- **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.
- **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.
- **T. Shaska and V. Ustimenko**, *On the homogeneous algebraic graphs of large girth and their applications*, Linear Algebra Appl., 430 (2009), no. 7, 1826–1837.
- **T. Shaska and V. Ustimenko**, *On some applications of graphs to cryptography and turbocoding*, Albanian J. Math., Vol 2, Nr. 3, 2008, 249 – 255..
- **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.
- **T. Shaska**, *Quantum codes from algebraic curves with automorphisms*, Condensed Matter Physics, Vol. 11, 2008, No 2 (54), 383-396..
- **T. Shaska and R. Sanjeewa**, *Determining equations of families of cyclic curves*, Albanian J. Math., Vol 2, Nr. 3, 2008, 199-213.
- **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.
- **T. Shaska and G. Wijesiri**, *Codes over rings of size four, Hermitian lattices, and corresponding theta functions*, Proc. Amer.Math. Soc., 136 (2008), no.3, 849-857.
<https://doi.org/10.1090/S0002-9939-07-09152-6>
- **E. Previato, T. Shaska, G. Wijesiri**, *Thetanulls of cyclic curves of small genus*, Albanian J. Math., vol. 1, Nr. 4, 2007, 253-270.
- **T. Shaska**, *Some open problems in computational algebraic geometry*, Albanian J. Math, vol I, Nr. 3, 2007, 297-319.
- **T. Shaska and Q. Wang**, *Automorphism groups of AG-codes based on C_{ab} curves*, Serdica J. Computing, Vol.1, Nr. 1, 2007, 193-206.
- **T. Shaska**, *Hyperelliptic curves with reduced automorphism group A_5* , Appl. Algebra Engrg. Comm. Comput., vol. 18, Nr. 1-2, 2007, pg. 3-20.
- **T. Shaska**, *Subvarieties of the hyperelliptic moduli determined by group actions*, Serdica Math. Journal, No. 4, (2006), 355-374.
- **J. Gutierrez and T. Shaska**, *Hyperelliptic curves with extra involutions*, LMS J. of Comp. Math., 8, (2005), 102-115. .
DOI: <https://doi.org/10.1112/S1461157000000917>
- **T. Shaska**, *Some special families of hyperelliptic curves*, J. Algebra Appl., 3 (2004), no. 1, 75–89.
- **T. Shaska**, *Genus 2 fields with degree 3 elliptic subfields*, Forum Math., 16 (2004), no. 2, 263–280.
<https://www.degruyter.com/view/j/form.2004.16.issue-2/form.2004.013/form.2004.013.xml>
- **K. Magaard, T. Shaska, S. Shpectorov, H. Völklein**, *The locus of curves with prescribed automorphism group*, Communications in arithmetic fundamental groups (Kyoto, 1999/2001). Sūrikaiseikikenkyūsho Kōkyūroku, No. 1267 (2002), 112–141.
- **T. Shaska**, *Curves of Genus 2 with (n, n) Decomposable Jacobians*, Jour. Symb. Comp., vol.31, No.5, pg. 603- 617, 2001.

Conference Proceedings

- **G. Frey and T. Shaska**, *Curves, Jacobians, and Cryptography*, Contemporary Math., vol. 724, 2019, pg. 279-345..
- **A. Broughton, A. Wootton, T. Shaska**, *On automorphisms of algebraic curves*, Contemporary Math., vol. 724, 2019, pg. 175-212..
- **Shuichi Otake and Tony Shaska**, *Bezoutians and the discriminant of a certain quadrimials*, Contemporary Math., vol. 724, 2019, pg. 55-72..
- **J. Mandili and T. Shaska**, *Heights on weighted projective spaces*, Contemporary Math., vol. 724, 2019, pg. 149-160..
- **R. Hidalgo and T. Shaska**, *On the field of moduli of superelliptic curves*, Contemporary Math., vol. 703, 2018, 49-64.
- **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, 2018, 87-120.
- **D. Joyner and T. Shaska**, *Self-inversive polynomials, curves, and codes*, Contemporary Math., vol. 703, 2018, 197 - 218.
- **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, 2015, 47–69.
- **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, 2015, 259–298 .
- **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, 2015..
- **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, 2011..
- **L. Beshaj and T. Shaska**, *Decomposition of some Jacobian varieties of dimension 3*, Artificial Intelligence and Symbolic Computation, LNCS vol. 8884, 193-204.
- **L. Beshaj, T. Shaska, C. Shor**, *On Jacobians of curves with superelliptic components*, Contemp. Math., vol. 29, 2014, 1–14.
- **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..
- **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.
- **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.
- **A. Bialostocki and T. Shaska**, *Galois groups of prime degree polynomials with nonreal roots*, Lect. Notes in Computing, 13, 2005, 243–255.
- **J. Gutierrez, T. Shaska, D. Sevilla**, *Hyperelliptic curves of genus 3 with prescribed automorphism groups*, Lect. Notes Comp., vol 13. (2005), 109–123.
- **V. Krishnamoorthy, T. Shaska, H. Voelklein**, *Invariants of binary forms*, Dev. in Math., vol 12, pg.101-122, Springer, 2005.
- **T. Shaska**, *Genus 2 curves covering elliptic curves: a computational approach*, Lect. Notes in Comp., vol 13. (2005), 205-231.
- **T. Shaska**, *Computational Aspects of Hyperelliptic Curves*, Computer Mathematics, Lecture Notes Ser. Comput. 10, 248–257, World Sci. Publishing, River Edge, NJ. .
- **T. Shaska and J. Thompson**, *On the generic curve of genus 3*, Contemporary Math., vol. 369, pg. 233-244, AMS, 2005.

- **T. Shaska and H. Voelklein**, *Elliptic subfields and automorphisms of genus 2 function fields*, Algebra, arithmetic and geometry with applications, Springer, 2004, 703–723.
- **T. Shaska**, *Determining the automorphism group of a hyperelliptic curve*, International Symposium on Symbolic and Algebraic Computation, ISSAC 03, New York, 2003, 248–254.
- **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.

Selected talks

- November 2019 [The arithmetic of weighted moduli spaces](#), NATO Advanced Study Institute: Recent trends in cryptology and cyber security, Kyiv, Ukraine, May 2020
- May 2020 [Addition on Jacobian varieties from a geometric viewpoint](#), National University of Greece, Athens, Greece.
- April 2019 [Abelian varieties with complex multiplication](#), Explicit Methods for Abelian and Calabi-Yau varieties, Utah State University, Logan, UT.
- April 2019 [Isogenies of 2-dimensional Jacobians](#), Mathematical Cryptology, Spring Eastern Sectional Meeting University of Connecticut Hartford, Hartford, CT
- March 2019 [Curves, automorphisms, and their Jacobians](#), Algebra seminar, College of Charleston, Charleston, SC.
- February 2019 [Superelliptic curves with complex multiplication](#), Special session: Automorphisms of curves, Santander, Spain.
- November 2018 [Heights on weighted projective spaces](#), Algebra Seminar, Wayne State University, Detroit, MI.
- October 2018 [Heights on weighted projective spaces](#), AMS Special Session: From hyperelliptic to superelliptic curves, Ann Arbor, MI.
- August 2018 [Abelian Varieties and Cryptography](#), Algebraic Curves, Integrable Systems, and Cryptography, National University of Kyiv-Mohyla Academy, Kiev, Ukraine
- April 2018 [The group law for the Jacobi variety of a hyperelliptic curves](#), Utah State, Logan, Utah
- April 2018 [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. April 14-15, 2018.
- March 2018 [Isogenies of Abelian varieties](#), Algebraic curves and their applications, AMS Sectional Meeting in Columbus, OH. March 17-18, 2018.
- September 2017 [From hyperelliptic to superelliptic curves](#), Algebraic curves and their applications, AMS Sectional Meeting in Orlando, FL. September 22-23, 2017.
- April 2017 [From hyperelliptic to superelliptic curves](#), Department of Mathematics, US Naval Academy, April 22, 2017.
- January 2017 [A pair of universal curves of genus 2](#), AMS Joint Meeting in Atlanta, GA. January, 4-7, 2017.
- October 2015 [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, 2015
- October 2015 [Julia quadratic of superelliptic Riemann surfaces](#), AMS Special Session on Riemann surfaces and their automorphisms, Chicago, Oct. 3-4, 2015
- June 2015 [Integral minimal models for binary forms](#), Mathematics Colloquium, University of Florida, Gainesville.
- March 2015 [Binary forms of minimal height](#), AMS Sectional Meeting, East Lansing
- July 2014 [Heights on algebraic curves](#), NATO ASI, Ohrid, 2015
- July 2014 [Minimal models for curves over their minimal field of definition](#), ACA 2014, New York.
- July 2014 [Genus 3 hyperelliptic curves with \(2, 4, 4\) split Jacobians](#), ACA 2014, New York.
- March 2014 [Minimal equations of curves over their minimal field of definition](#), Southeastern Spring Sectional Meeting University of Tennessee, Knoxville, Meeting #1097
- June 2013 [Decomposition of Jacobians of superelliptic curves](#), Riemann and Klein Surfaces, Symmetries and Moduli Spaces, Linkoping, Sweden
- April 2013 [Automorphisms of curves and their Jacobians](#), AMS Special Session on Computational Advances on Special Functions and Tropical Geometry, Iowa State University

- May 2013 [Stratifications on moduli spaces of curves and superelliptic loci](#), MCAG 2013, Western Michigan University
- March 2013 [Genus 3 hyperelliptic curves with split Jacobians and many rational points](#), Mathematics Colloquium, Georgia Southern University
- Nov. 2012 [Some remarks on binary octavics](#), Mathematics Colloquium, Michigan Tech. University
- Nov. 2012 [Some remarks on binary octavics](#), Mathematics Colloquium, Cleveland State University
- Oct. 2012 [An introduction to the invariant theory of binary forms](#), Mathematics Colloquium, Duquesne University
- June 2012 [A historical view of theta functions](#) (plenary talk), Conference on Applications of Algebra, Yildiz University, Istanbul, Turkey
- March 2012 [Thetanulls of algebraic curves and some applications](#), AMS Special session on Computational Algebraic Geometry, Tampa, Florida
- Jan 2012 [Interesting families of algebraic curves](#), Joint AMS Meeting, Special Session on Mathematics of Computation, Boston
- Jan. 2012 [Half-integer theta-nulls of superelliptic curves](#), AMS Sectional Meeting: Special Session on Computational and Algorithmic Algebraic Geometry, Salt Lake City
- Oct. 2011 [Theta Functions of algebraic curves](#), Special Session on theta functions, SIAM National Conference, Raleigh
- July 2011 [Computational aspects of low genus curves](#), Laurier Centennial Conference: AMMCS-2011, Waterloo
- May 2011 [Theta-nulls of algebraic curves](#), 10th Panhellenic Geometry Conference, Patras, Greece
- Nov. 2010 [Hybrid Methodologies for Symbolic-Numeric Computation](#), MSRI, Berkeley
- Oct. 2009 [Automorphism groups of superelliptic curves](#), Workshop on Mathematical Cryptology, University of Cantabria, Spain
- March 2008 [Theta functions in coding theory](#), Mathematics Colloquium, University of Delaware
- Oct. 2007 [Genus 2 curves covering elliptic curves](#), Mathematics Colloquium, Simon Fraser University, Vancouver
- Oct. 2007 [Equations of curves with automorphisms](#), AMS Sectional Meeting, Special Session on Numerical and Symbolic Techniques in Algebraic Geometry and Its Applications, DePaul University
- Sep. 2007 [Remarks on some old problems of algebraic geometry](#), Mathematics Colloquium, Michigan Tech.
- May 2007 [A historical view of theta functions](#), Mathematics Colloquium, Lublin, Poland
- Aug. 2006 [Codes over rings of size four, lattices, and their theta functions](#), Mathematics Colloquium, Lublin, Poland
- Oct. 2006 [Some open problems in computational geometry](#), Mathematics Colloquium, University of Michigan-Dearborn
- May 2006 [Theta functions and automorphism groups of curves](#), Galoistheorie Kolloquium, Institut für Experimentelle Mathematik (IEM), Essen, Germany
- June 2006 [Theta functions and application to coding theory](#), (ACA 2006), Varna, Bulgaria
- April 2005 [Hyperelliptic curves with reduced automorphism group \$A_5\$](#) , AMS Western section, Santa Barbara
- Jan. 2005 [Genus 2 curves that admit a degree 5 map to an elliptic curve](#), Joint AMS meeting, Atlanta
- Dec. 2004 [Genus 2 curves with \(5, 5\) split Jacobian](#), Institute for Experimental Mathematics, Essen, Germany
- July. 2004 [Field of moduli of curves, a computational approach](#), Workshop Computational Arithmetic Geometry, PIMS Simon Fraiser University, Vancouver
- Oct. 2003 [Genus 2 curves with degree 5 elliptic subcovers](#), 991-14-21 AMS, Southeastern Section Meeting, Chapel Hill
- Aug. 2003 [Determining the automorphism group of algebraic curves](#), ISSAC 03, Drexler University, Philadelphia
- Jul. 2003 [Computational aspects of hyperelliptic curves](#), ACA 03, Raleigh, NC
- June 2003 [The monodromy group of a generic curve covering \$\mathbb{P}^1\$](#) , Joint International Meeting of AMS and RSME, Seville, Spain
- June 2003 [Computational aspects of hyperelliptic curves](#), University of Cantabria, Santander, Spain
- Oct. 2003 [Loci of hyperelliptic curves with prescribed group action](#), Computational Aspects of Algebraic Curves, and Cryptography, Gainesville

- Jan. 2003 [Hyperelliptic curves with non-hyperelliptic involutions](#) 983-14-115 AMS, JMN, Baltimore
- Sep. 2002 [Hyperelliptic curves with extra automorphisms](#), Galois Theory Conference, John Thompson's 70th birthday, University of Florida, Gainesville
- Sep. 2002 [Field of definition and field of moduli of hyperelliptic curves](#), University of Florida Colloquium, Gainesville, Florida
- Dec. 2002 [Computational aspects of algebraic geometry](#), Algebra seminar, UC Irvine, Irvine, CA
- Jul. 2002 [Genus 2 curves with \(3,3\)-split Jacobian and large automorphism group](#), ANTS V, International Symposium in Algorithmic Number Theory, Sydney, Australia
- Nov. 2001 [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. 2001 [The automorphism group of a Riemann surface](#), University of Florida Colloquium, Gainesville, Florida
- June 2001 [Elliptic subfields and automorphisms of genus 2 curves](#), University of Erlangen, Germany
- May 2001 [Computing the locus of genus 2 fields with degree 2 or 3 elliptic subfields](#), Institute for Experimental Mathematics, Essen, Germany
- May 2001 [Some Computational Aspects of Genus 2 Curves](#), Number Theory Conference, University of Illinois, Urbana-Champaign, IL
- Dec. 2000 [Genus 2 curves covering elliptic curves](#), Workshop on Arithmetic Geometry, MSRI, Berkeley, CA
- June. 2000 [Modular curves and Hurwitz spaces](#), Conference on Topological Groups, TU-München, Germany
- March 2000 [Curves of genus two with \(n,n\)-decomposable Jacobians](#), AG Gruppentheorie, Erlangen, Germany
- May 1999 [Explicit equation of certain Hurwitz spaces](#), University of Heidelberg, Germany

Conferences Organized

- December 2018 [Tirana Winter School in Algebraic Geometry](#), Tiranë, Albania, December 28-29, 2018.
- October 2018 [From hyperelliptic to superelliptic curves](#), Spring Central Sectional Meetings in University of Michigan, Meeting 1143. (with Yuri Zarhin and Nicola Tarasca)
- August 2018 [Algebraic Curves, Integrable Systems, Cryptography](#) (with Julia Bernatska and Victor Enolski), Kiev, Ukraine, August 24-25, 2018
- March 2018 [Arithmetic of Algebraic Curves](#), Spring Central Sectional Meetings in Ohio State University, Meeting 1136. (with A. Elezi and M. Polak)
- Jan, 2017 [Minimal integral models of algebraic curves](#), AMS Joint Meeting, January 2017, Atlanta, GA.
- Nov. 2016 [Varieties, their fibrations and automorphisms in mathematical physics and arithmetic geometry](#), AMS Sectional Meeting, November 2016, Raleigh, NC.
- January 2016 [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, January 6-9, 2016
- March 2015 Special Session: Arithmetic of Hyperelliptic Curves, Michigan State University, East Lansing, MI.
- August 2014 [Nato Advanced Study Institute](#), Arithmetic of Hyperelliptic Curves, Ohrid, Macedonia.
T. Shaska, E. Zhupa
- July 2014 [Applications of Computer Algebra \(ACA 2014\)](#), Fordham University, New York. R. H. Lewis, T. Shaska
2014 Co-organizer: Moduli spaces and arithmetic dynamics, Special Session, ACA 2014, Fordham, New York, July 9-12, 2014
- July 2013 [Arithmetic of algebraic curves](#), ACA 2013, Malaga, Spain. (with J. M. Couveignes, N. Pagani)
- June 2012 MCAG 2012: [Michigan Computational Algebraic Geometry 2012](#), Oakland University, Rochester, MI.
Tony Shaska, Dan Erman, Charles Wampler
- June 2012 ECCAD 2012: East Coast Computer Algebra Day, Oakland University, Rochester, MI.
T. Shaska, D. Steffy
- Mar. 2012 Special Session: Computational Algebraic Geometry, AMS Sectional Meeting, Tampa, FL.
A. Elezi, T. Shaska

- Jan. 2011 Computational Algebraic and Analytic, Geometry for Low-Dimensional Varieties. AMS Annual Meeting, New Orleans (with M. Seppala, E. Volchek)
- June 2010 General Chair: Applications of Computer Algebra, ACA 2010, June 24-27, 2010, University of Vlora, supported by Ministry of Science and Education, Albania.
T. Shaska, E. Ruci, E. Zhupa, J. Calmet, A. Akritas, M. Wester
- Jan. 2009 Special Session: 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 2007 [Conference in algebra, coding theory, and cryptography](#), Vlora, Albania.
A. Elezi, T. Shaska
- July 2007 Applications of Computer Algebra, ACA 2007, Oakland University, Rochester, MI.
- July 2007 Special session: [Coding theory and cryptography](#), ACA 2007, Rochester, MI.
D. Joyner, T. Shaska, C. Shor
- July 2007 Special session: Computational algebraic geometry, ACA 2007, Rochester, MI.
A. Elezi, T. Shaska
- Jan. 2007 Special Session: Computational Algebraic and Analytic, Geometry for Low-Dimensional Varieties. AMS Annual Meeting, New Orleans (M. Seppala, E. Volchek)
- June 2006 Special Session: Coding theory and cryptography, ACA 2006, Varna, Bulgaria. (with S. Dodunekov)
- May 2005 Computational aspects of algebraic curves, University of Idaho, Moscow, Idaho, 2005.
- Jan. 2005 *Special Session: Algorithmic Algebraic and Analytic Geometry*, AMS Annual Meeting, Atlanta, GA. (with M. Seppala, E. Volchek)
- July 2004 Special session: *Computational aspects of algebraic curves*, ACA 2004, Beaumont, TX.
- July 2003 Special session: [Computational aspects of algebraic curves](#), ACA 2003, NC State, Raleigh, NC.

Grants

- 2014 **Nato Advanced Study Institute**, Hyperelliptic Curve Cryptography.
ISEG. EAP.ASI 984724, €80 000
- 2012 **National Security Agency**, *Conference Grant*, Oakland University, NSA # H982301210275, \$20 000.
- 2012 **Office of Provost**, *Michigan Computational Algebraic Geometry*, Oakland University, \$5 000.
- 2007-10 **National Science Foundation**, *REU*, Oakland University, Co-PI: \$342 899.
- 2008 **Nato Advanced Study Institute**, *New challenges in digital communications*, ICS.EAP.ASI 982903, €85 200.
- 2007 **National Science Foundation**, *Applications of Computer Algebra*, Oakland University, \$20 000.
- 2005 **National Security Agency**, *Computational Aspects of Algebraic Curves*, Univ. of Idaho, \$12 000.
- 2004 **National Science Foundation**, *NSF-Epscor S0-511*, University of Idaho, NSF, \$15 000.
- 2000 **Deutsche Forschungsgemeinschaft**, *Friedrich-Alexander-Universität Erlangen-Nürnberg*, DM 24000.
- 2001 **Threadgill Dissertation**, *Department of Mathematics*, University of Florida, Gainesville, FL.

Service

Reviewer for MathSciNet (40 articles reviewed)

Committees

2010–2013 *Committee on Human Rights, American Mathematical Society*

Ph.D. students

Current students

2019-present **D. Tabaku**, *Oakland University*.

Former students

- 2011-2016 **L. Beshaj**, *Ph.D. Mathematics*, Oakland University.
 Thesis: Integral binary forms with minimal height
 Position: Assistant Professor, Army Cyber Institute, West Point Military Academy
- 2005-2009 **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
- 2005-2008 **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 [Computational Algebra, MTH 5777](#): Fall 2019
[Theory of Computation , APM 5881](#): Fall 2019
[Algebraic Geometry, MTH 6772](#)
[Algebraic Number Theory, MTH 6771](#)
[Commutative Algebra, MTH 6770](#):
[Algebra I-II, MTH 5771-5772](#):
[Computational Algebra, MTH 5777](#):
[Coding Theory, APM 6773](#):
[Algebraic Topology](#):
[Abstract Algebra, MTH 475-476](#):
[Geometry, MTH 462](#)
[Linear Algebra, APM 2775](#)
[Logic and Proofs, MTH 3002](#)
[Calculus I, II, III](#)
[Cryptosystems in Automotive Industry, MTH 505](#) Fall 2015
 Special Topics: Algebraic geometry methods in engineering, Summer 2006
 Special Topics: Topics in Cryptology, APM 505, Summer 05
 Discrete Mathematics, APM 2663
 Graph Theory and Combinatorial Math, APM 5663
- University of Idaho [Computer Security and Cryptography, Math 504](#), Spring 05
[Galois Theory, Math 553](#), Spring 2004
[Group Theory, Math 552](#), Fall 2003
[Linear Algebra, Math 330](#), Spring, Summer, Fall 04
[Abstract Algebra, Math 461](#), Fall 04
[Introduction to Cryptography, Math 435](#), Spring 05
- UC Irvine [Calculus I, II](#),
[Infinite Series and Complex Numbers](#),
[Elementary Linear Algebra](#),
[Linear Algebra I, II](#),
- University of Florida [Calculus I, II](#),
[Linear Algebra](#),
[Differential Equations](#),

References

Ron Donagi, *Professor of Mathematics*, University of Pennsylvania.
 Email: donagi@math.upenn.edu

Emma Previato, *Professor of Mathematics*, Boston University.

Email: ep@math.bu.edu

Mike Fried, *Retired Professor of Mathematics*, UC Irvinet.

Email: michaeldavidfried@gmail.com

Fioralba Cakoni, *Professor of Mathematics*, Rutgers University.

Email: fc292@math.rutgers.edu

Nigel Boston, *Professor of Mathematics*, University of Wisconsin – Madison.

Email: boston@math.wisc.edu