SARAH ARPIN

sarah.arpin@colorado.edu
http://math.colorado.edu/~saar7867/
University of Colorado Boulder
Boulder, CO

RESEARCH AREAS

Algebraic number theory, supersingular elliptic curve isogeny graphs, isogeny-based cryptography, quantum cryptography, arithmetic geometry in characteristic p, linear codes.

EDUCATION

PhD	University of Colorado Boulder, Pure Mathematics Number Theory Advisor: Dr. Katherine E. Stange	Expected Spring 2022
MS	University of Colorado Boulder, Applied Mathematics Completed as work towards Ph.D. in Pure Mathematics	April 2019
MA	CUNY Hunter College, Pure Mathematics Completed as work towards Ph.D. in Pure Mathematics	April 2012
BA	Sarah Lawrence College, B.A. in Liberal Arts Concentrated in Mathematics	May 2008

PUBLICATIONS

Journal Papers Accepted

S. Arpin, C. Camacho-Navarro, K. Lauter, J. Lim, K. Nelson, T. Scholl, J. Sotáková. "Adventures in supersingularland." *Experimental Mathematics*, 2021. https://doi.org/10.1080/10586458.2021.1926009. First appeared: September 2019.

Journal Papers in Review

S. Arpin, R. Griffon, L. Taylor, N. Triantafillou. "On the arithmetic of a twisted constant family of superelliptic curves," Submitted. https://arxiv.org/abs/2105.02812 First appeared: May 2021.

Preprints

S. Arpin, S. Bozlee, L. Herr, H. Smith. "The scheme of monogenic generators and its twists." https://arxiv.org/abs/2108.07185 First appeared: August 2021.

RESEARCH EXPERIENCE

University of Colorado Boulder Summer 2017
Summer Research Assistant

- Completed research on algebraic number theory problems relating to the Ring Learning With Errors (RLWE) cryptographic protocol. Under the direction of Dr. Katherine E. Stange.

University of Colorado Boulder Experimental Mathematics Lab 2018-2021
Graduate Student Mentor

- Graduate student mentor on two separate experimental math lab projects, each for one academic year. *Binomial Transformation* and *Mathematics of COVID-19*

PRESENTATIONS

Invited

Seminar Presentation, "Adding Level Structure to Supersingular Elliptic Curve Isogeny Graphs," Ohio State University Number Theory Seminar. November 22nd, 2021. [Upcoming]

Seminar Presentation, "Adding Level Structure to Supersingular Elliptic Curve Isogeny Graphs," University of California Irvine Number Theory Seminar. October 14th, 2021.

Seminar Presentation, "An Exploration of Supersingular Elliptic Curve Isogeny Graphs," University of California Davis Number Theory Seminar. May 13th, 2021.

Conference Presentation, "An Exploration of Supersingular Elliptic Curve Isogeny Graphs," Joint Mathematics Meeting. January 9th, 2021.

Contributed

Poster, "On the arithmetic of a twisted constant family of superelliptic curves," Western Algebraic Geometry Symposium. University of Utah, Salt Lake City, UT. November 2-3, 2019.

Conference Presentation, "An Exploration of Supersingular Elliptic Curve Isogeny Graphs," Number Theory Series LA. Occidental College, Los Angeles, CA. October 26-27, 2019.

Conference Presentation, "On Ring Learning With Errors," Joint Mathematics Meeting. January, 2018.

TEACHING EXPERIENCE

University of Colorado Boulder, Boulder, CO August 2016 to present
Graduate Student TA/RA, Mathematics Department

- In courses taught as instructor, responsibilities included: Developing lecture material and quizzes, three or four in-class hours with students per week, weekly office hours, grading and contributing to writing exams. Class sizes: ~30.
- In courses taught as teaching assistant, responsibilities included: Leading weekly problem sessions with students, grading and providing feedback on homework, weekly hours in the CU Boulder mathematics tutoring center.
- Experience instructing via Zoom.
- In Fall 2021, I held an RA-ship to focus on my dissertation research.

Courses Taught as Instructor
Math 2510: Introduction to Statistics, Spring 2021 (taught remotely)
Math 1300: Calculus I, Fall 2020 (taught remotely)
Math 2300: Calculus II, Fall and Spring 2019
Math 1310: Calculus for Life Sciences: Fall and Spring 2018

Courses Taught as Teaching Assistant
Math 2400: Calculus III, Spring 2020
Math 1310: Calculus for Life Sciences, Fall 2017
Math 1300: Calculus I, Spring 2017
Math 1011: College Algebra, Fall 2016

CUNY Hunter College, New York City, N.Y. May 2011 to August 2016
Adjunct Lecturer, Department of Mathematics and Statistics

- Responsibilities included course design and development of lecture materials, quizzes, and exams. All grading responsibilities. Collaborated with the department chair to develop the complete curriculum of the Axiomatic Geometry course.

Courses Taught as Instructor
Pre-Calculus, Calculus I, Calculus III, Matrix Algebra, Number Theory, Axiomatic Geometry

Mercy College, Dobbs Ferry, N.Y. August 2014 to August 2016
Adjunct Lecturer, Department of Mathematics and Computer Sciences

- Responsibilities included course design and development of lecture materials, quizzes, and exams.

Courses Taught as Instructor
College Algebra

WORKSHOP PARTICIPATION

Supersingular Isogeny Graphs in Cryptography
BIRS, Banff, CA, Summer 2021
Invited workshop participant. Workshop held virtually, supported by BIRS.

Rethinking Number Theory 2
Virtual Conference, Summer 2021
Selected workshop participant for the *Linear Codes: BIKE* working group led by Angela Robinson (NIST).

Women in Numbers 5
BIRS, Banff, CA, Summer 2021
Selected workshop participant in the isogeny-based cryptography working group led by Kristin Lauter (Facebook AI Research) and Katherine Stange. Workshop held virtually.

Sage Days 103: Women in Sage
St. Louis, MI, 2019
Selected workshop participant.

Explicit Methods in Arithmetic Geometry in Characteristic *p*
Mathematics Research Community, Whispering Pines, RI, Summer 2019
Selected workshop participant.

Visitor to Microsoft Research
Microsoft Research, Bellevue, WA, June 2019
Invited researcher, hosted by Kristin Lauter and the Cryptography Research Group.

Open Questions in Cryptography and Number Theory
University of California Irvine, Irvine, CA, September 2018
Workshop participant in the working group led by Kristin Lauter.

Connecticut Summer School in Number Theory
University of Connecticut, Storrs, CT. Summer 2018
Selected workshop and conference participant.

Graduate Workshop in Algebraic Geometry for Women and Mathematicians of Minority Genders
MIT & Harvard, Boston, Mass., February 2018
Selected workshop participant.

PROFESSIONAL SERVICE

Conference Co-Organizer
Front Range Number Theory Day, Colorado.
FRNTD is a twice-yearly NSF-sponsored regional conference whose goal is to bring together number theorists in the Front Range region of the United States. The conference is held alternately at CU Boulder and CSU Fort Collins. I have been a graduate student co-organizer since 2019.

Special Session Co-Organizer
Joint Mathematics Meetings 2020, Denver, CO.
I co-organized the special session from the Mathematics Research Community "Explicit Methods in Arithmetic Geometry in Characteristic *p*."

COMMUNITY SERVICE

CU Boulder Mathematics Department Diversity Committee
Active member since 2016

CU Boulder Mathematics Department Peer Mentorship Program
Founding lead mentor since 2019

CU Boulder Mathematics Department Graduate Student Representative
Elected graduate student representative to the graduate committee, and served for the academic years 2018-20

CU Boulder STEMinar
Co-organizer since 2018

OTHER

U.S. Citizen

Languages

English: Native Language

French: Novice Listener and Speaker, Intermediate Reading and Writing

Computer Skills

Programming: Python

Applications: SageMath, Magma