ChatGPT
The mathematics behind the global AI phenomenon

POST-QUANTUM CRYPTOGRAPHY
The latest cybersecurity measures

A LEGEND RETIRES
James Arthur gives his last graduate course

CHANGING THE EQUATION
Vanessa Vakharia wants to redefine failure in the math classroom
MISSION STATEMENT
At the Fields Institute, mathematics research, innovation and education flourish. We foster an inclusive, equitable and collaborative culture where everyone can discover mathematics, and where mathematicians make meaningful contributions to the world.

**Fields Notes, The Fields Institute for Research in Mathematical Sciences**
Director: **Kumar Murty**
Deputy Director: **Deirdre Haskell**
Managing Editor: **Jordana Feldman**
Contributing Writers: Chantal Buteau, Aaron Crighton, Pamela Brittain, Dragana Martinovic, Alik Sokolov, Vanessa Vakharia

**QUESTIONS? COMMENTS?** We love to hear from you.
Email: communications@fields.utoronto.ca
Connect with Fields!
CONTENTS

2 Upcoming Opportunities

3 Kumar Murty wins the 2023 CMS Jeffery-Williams Prize

4 2023 Thematic and Focus Programs Calendar

5 Leaving Far More Than a Trace

8 Life @ Fields

10 2022 Fields Medal Symposium: Akshay Venkatesh

12 Postdoc Spotlight: Sharmila Gunasekaran

14 2023 Fields Medal Symposium preview

21 Uncertainty Principle: Post-Quantum Cryptography is the Key to a More Cyber-Secure Future

24 Vanessa Vakharia: Redefining Failure in the Classroom

26 Getting Elementary Classrooms Cyber-ready

27 Farewell to the Math Knowledge Network

28 Fields of Dreams: Therese Landry

30 Award Winners: Christian Genest, Lynda Colgan

32 Partners & Sponsors

SPRING | SUMMER 2023
Fields Research Fellowships
Faculty and researchers from our Principal Sponsoring Universities are invited to apply for this full-time research opportunity at Fields or to nominate a visiting mathematical scientist on their behalf.

Application deadlines: January 15, May 15 and September 15 of each calendar year.

Simons Distinguished Visitorship
This prestigious six-month appointment will provide a world-renowned researcher with a unique opportunity to work at the Fields Institute with many Canadian and international colleagues on a research project of their choosing.

Application details will be available in Fall 2023.

Dean’s Distinguished Visiting Professorship
A joint program of the Fields Institute and select Principal Sponsoring Universities, the Dean’s Distinguished Visiting Professorship brings leading international researchers in the mathematical sciences to the Fields Institute to be in residence for a term. Currently, we have two annual positions: one with McMaster University and one with the University of Toronto.

By nomination only. Please check the Fields website for more details.

CRM-Fields-PIMS Prize
The CRM-Fields-PIMS prize is the premier Canadian award for research achievements in the mathematical sciences. It is awarded jointly by the three Canadian mathematics institutes.

Nomination deadline: Fall 2023.

The Margaret Sinclair Memorial Award Recognizing Innovation and Excellence in Mathematics Education
This award recognizes an educator in Canada who has demonstrated innovation and excellence in promoting mathematics education at the elementary, secondary, college or university level.

The Fields Institute is proud to share that our director, V. Kumar Murty, has made additional space on his shelf for the 2023 CMS Jeffery-Williams Prize. Murty received the award for his contributions to mathematical research and will deliver a lecture in Ottawa this June at the 2023 CMS Summer Meeting.

The Jeffery-Williams Prize is named after Ralph Jeffery and Lloyd Williams, two influential Canadian mathematicians. The American-born Williams founded the Canadian Mathematical Congress in 1945, which later became the Canadian Mathematical Society, and is known for overseeing the doctorate of Elbert Frank Cox, the first Black person to receive a PhD in mathematics. A Nova Scotia native, Jeffery is known for his contributions to integration theory. Students at Queen’s University, where he taught, will also recognize his name from Jeffery Hall.

The award in their name has been handed out since 1968 to a notable Canadian mathematician. Winners join a formidable group of past recipients, which includes Cathleen Synge Morawetz, Robert Langlands, James Arthur, Donald Coxeter and founding Fields Institute Director, Jerrold E. Marsden.

“I am delighted and thankful to the Canadian Mathematics Society for this recognition. It’s good to know that one’s work is appreciated. At the same time, it is also humbling, given the list of distinguished past winners of the prize,” Murty said.

Murty was singled out for the diversity of his mathematical interests in fundamental research, but also for his interest in applying this research outside of academic settings. Known primarily as a number theorist, he has contributed to arithmetic algebraic geometry, analytic number theory, algebraic number theory and information security. More recently, he has made forays into the world of “mathematics for a better world” through his work on integrative modelling related to the COVID-19 pandemic, climate change and Smart Villages – a particular passion project.

At the onset of the COVID-19 outbreak in Canada, Murty led a team that was consulted by the Ontario government to help inform policy decisions. Together with Fields Fellow and Scotiabank’s leading data scientist, Taha Jaffer, he developed the Hurricane model and used it as an early predictor of pandemic dynamics. Hurricane models are part of the nonparametric family of models that are typically found in finance and apply well to the cyclical nature of case trend transitioning between quadrants of growth and change in growth.

Thanks to the success of these results and Murty’s early initiative, Fields spearheaded the Mathematical Modelling of COVID-19 Task Force, which unified dozens of epidemiologists, math modellers and infectious disease experts across the country and has since expanded into Mathematics for Public Health (MfPH), a pan-Canadian network that can rapidly respond to public health emergencies.

Known as a “galaxy brain” around the Institute for his ability to envision large-scale and far-reaching projects, Murty has also established Fields Multiplier, an initiative that provides support for mathematics-based research and development with high potential for commercialization.

Murty was nominated by previous winner, George Elliott. “I am happy to see my colleague’s work in number theory and arithmetic geometry recognized with this prestigious award. He has made important contributions over many years, both scientifically, and in general to the discipline,” he said.
2023 THEMATIC AND FOCUS PROGRAMS CALENDAR

A list of upcoming events linked to our core programs

Thematic Program on Set-Theoretic Methods in Algebra, Dynamics and Geometry
January 1 – June 30, 2023

Mini-workshop on Set-Theoretic Methods in Module Theory and Homological Algebra
May 29 – June 2, 2023

Workshop on the Frontiers of Set Theory
June 5 – 9, 2023

Coxeter Lecture Series: Maryanthe Malliaris
May 29 – June 2, 2023

Thematic Program on Operator Algebras and Applications
July 1 – December 31, 2023

Workshop on Operator Algebras and Applications: Connections with Logic
August 28 – September 1, 2023

Graduate Course on K-Theory and C*-Algebras
September 11 – December 8, 2023

Workshop on Operator Algebras and Applications: Symmetry and Structure
September 18 – 22, 2023

Workshop on Operator Algebras and Applications: Groups and Group Actions
October 2 – 6, 2023

Twinned Conference on C*-Algebras and Tensor Categories
November 6 – 10, 2023

Workshop on Operator Algebras and Applications: Free Probability
November 13 – 17, 2023

Workshop on Operator Algebras and Applications: Non-Commutative Geometry
December 4 – 8, 2023

2023-2024 Operator Algebra Seminar
July 1, 2023 – June 30, 2024

Fields Undergraduate Summer Research Program (FUSRP)
June 12 – August 10, 2023

Research Projects:
On Field Extensions of Nonarchimedean Local Fields and Local Langlands Correspondence
Active Human-Centric Evaluations in NLP Interpretability
Statistical and Machine Learning and Applications
Spectral graph invariants and random walks on graphs
Bootstrapping the eigenvalues of discrete hyperbolic surfaces
Random multiplicative functions over function fields

Spectral-Spatial Tissue Boundary Detection in Biomedical Hyperspectral Images
Physiological feature extraction using facial video data

Focus Program on Geometric Constraint Systems
July 1 – August 31, 2023

Workshop on Geometric Constraints: Materials, Graphs and Matroids, Rigidity and Packings
July 10 – 14, 2023

Workshop on Constraint Systems: Distance Geometry, Structured Polynomials, Matrix Completion and Kinematics
August 8 – 11, 2023

Visit fields.utoronto.ca/calendar for full event listings.
James Arthur’s retirement from teaching means he can devote himself to proving the Langlands Program conjectures

On April 10, James Arthur collected his notes, put them in his bag and walked out of the Fields Institute. He headed to his office on the sixth floor of the University of Toronto’s Bahen Centre for Information Technology, conveniently located across the courtyard at the back of the building. Moments earlier, the renowned mathematician wrapped up the final lecture in his graduate course on Automorphic Forms and Representation Theory. The course was billed as an introduction to the Langlands Program, a series of conjectures that supply the internal structure connecting phenomena in geometry and number theory with representation theory. The Program, first proposed by Robert Langlands in 1967, is considered one of the most significant mathematical discoveries of the last century, even as its difficulty has sometimes led to misunderstanding among mathematicians.

James Arthur’s retirement from teaching is also significant. More than anyone, Arthur has worked to take the Langlands Program from conjecture to realization. Automorphic forms are considered the key to unifying huge areas of mathematics and Arthur is credited with placing the trace formula at the centre of his approach, thereby moving the Langlands program from conjecture towards its future resolution. Key to this is the so-called trace formula, on which Arthur is the world’s expert. Langlands always believed that the trace formula would be the most powerful tool that could be brought to bear on his conjectures. In Arthur’s hands, it has attained this status, having in the process been named the Arthur-Selberg trace formula after his contributions. Robert Langlands himself described Arthur, his former graduate student, as “the leading mathematician in Canada.” The next generation agrees. According to Arthur’s own graduate student, Clifton Cunningham, “he is the Langlands Program in Canada.”

Arthur’s retirement has not received a great deal of attention so far. There are two main reasons why. The first is that the Langlands Program is still sometimes regarded as exotic. It requires a new way of thinking that can present a barrier to other mathematicians, especially since it can be difficult to explain. The second reason is that Arthur himself is sometimes low-key and gets focused on his own work. “As a new grad student, you get excited about courses and conferences,” Cunningham says. “Jim’s advice was always stay home, write the papers, then go when you have something to say. That’s his approach to everything. He quietly produces amazing work on his own terms decade after decade and people notice. There’s volume to that quiet voice. It’s very effective.”

But people are, in fact, listening. When Fields Director, Kumar Murty, heard Arthur needed a classroom for his last University of Toronto course, he jumped at the chance to bring him to the Fields Institute. Murty considered it a rare opportunity for the Shared Graduate Courses Program, part of Fields Academy that opens up advanced graduate-level courses taught at any of our Principal Sponsoring Universities to qualified students across the
province and the world. “We have a responsibility to preserve – and
even grow – what Arthur has built up. We at Fields, sitting right beside
the University of Toronto, have to see how we can continue the study
and develop this expertise,” Murty explains, before diving further
into the Fields ethos. “Canada has invested a lot in research and we
have the world’s leading expert on this really important subject. Fields
wants to make sure that knowledge becomes freely available and stimulates more research.”

Lightning in a bottle

Part of what makes the Langlands Program so important is that it
supplies the internal structure of some of the greatest phenomena
discovered in algebraic geometry, number theory and representation
theory. These fields were largely regarded as separate, but Langlands’
tunities linked them.

Langlands caused a stir when he first presented these ideas in 1967, and
it garnered him the kind of notice reserved for giants such as Alexander
Grothendieck. To understand the magnitude of his work, it’s important
to begin with a phenomenon in math research where two things that
at first seem like they shouldn’t be connected are, in fact, very much
connected. From this realization, amazing things can happen. One early example of this comes from Gauss. Today, the law of quadratic reciprocity is taught in a first course in elementary number theory, but it wasn’t always the case. Gauss was so mystified by this law, he gave eight
proofs trying to figure out why it was happening (and today there
are more than a hundred of them). But what remained mysterious
was why it was true and not just that it was true.

For the next 100 years, the subject of number theory continued to build on Gauss’s proofs in more and
more generality. Then, lightning in a bottle: Emil Artin published a
series of papers between 1924-1930 proving that an equality of certain
L-functions allows formulation of a generalization of quadratic reciprocity to n-dimensional representations. Quadratic reciprocity became the Artin reciprocity law, setting the stage for a related breakthrough several decades later.

Modern family of conjectures

When quadratic reciprocity became Artin reciprocity, mathematicians
already thought it was a big deal. Lightning in a bottle would strike again at the 1955 International
Symposium on Algebraic Number Theory in Japan. There, Yutaka
Taniyama presented what would become the Taniyama conjecture,
which he refined and corrected in 1957. It was further refined by Goro Shimura, while initial progress
toward proving it was later made by Andre Weil in 1967.

The Taniyama conjecture takes an elliptic curve from geometry.
It has an L-function associated with it $L(E, s)$. Taniyama conjectured
that there is an automorphic representation whose L-function
is the same as the L-function of the elliptic curve. The automorphic
representation is analysis, whereas the elliptic curve lies in the realm
of geometry. Here, Taniyama and Weil found a link between these two
disparate fields: they are connected through the intermediary of the
L-function. And this is a completely new reciprocity law.

After Weil’s work, Langlands changed everything at a famous conference in 1977. At the American Mathematical Society’s month-long Summer
Symposium in Corvallis, Oregon, he asserted that this sort of thing must
happen all the time – not just for the Taniyama conjecture. There must be
something more general. The elliptic curve is one of the first concrete
examples of what Grothendieck would call a motive. Langlands
said, why just this one motive?
They should all be connected to automorphic forms. Any motive has an L-function and that L-function should be the same as that of an automorphic representation.

With this intuition, and various other fundamental papers, Langlands linked his ideas to those of Grothendieck. These days, Langlands and Grothendieck are often compared for the historical influence their work will have. They are sometimes seen as the two greatest mathematicians of the second half of the twentieth century.

**Beyond Endoscopy**

In 1979, Langlands gave a series of lectures at the École normale supérieure de jeunes filles (later published as a book) on a new theory, now known as Endoscopy, which supplemented his 1967 conjectures. It postulated a refinement of the Arthur-Selberg trace formula, which he called the stable trace formula, and which would govern the finer properties of automorphic representations. In 2002, Arthur established the stable trace formula. This then served as the foundation for a project Arthur completed in 2013 that provides an endoscopic classification of the automorphic representations for many groups. His monograph on the subject remains the best progress to date of the Theory of Endoscopy.

Finally, around the year 2000, Langlands proposed a further theory, which he called Beyond Endoscopy. It outlines a strategy for using the stable trace formula to attack his original 1967 conjectures, and perhaps also his later conjecture on motives. As might be expected, this will be very difficult, requiring fundamental analytic and arithmetic questions that have never before been broached. Nevertheless, Arthur believes that Beyond Endoscopy represents the natural way to approach the Langlands conjectures and he is confident that it will eventually be solved.

**The message is in the motive**

This brings us back to Arthur’s Fields Institute lectures. The first two thirds of the course were a basic introduction to the Langlands program that largely followed Langlands’ 1969 Bochner paper in which he first outlined his conjectures. The remaining third delved into motives. Grothendieck’s idea of a motive is often regarded as his greatest mathematical insight, and one of the great achievements in pure abstract thought of any kind. He is said to have arrived at the name from the notion of a *motif* in music, art or literature – a fundamental hidden principle that governs what we hear, see or read. Arthur’s lectures on motives are largely speculative. They explore new ideas in the fundamental relationships between Grothendieck’s motives and Langlands’ automorphic representations.

Fields was honoured to host James Arthur’s final graduate class, and we offer the full course in video form on our YouTube channel. The hope is that he will continue to make use of our building, setting up an office where he can continue his important work and continue to inspire future generations of students and researchers. And one thing we can get better at in the meantime is promoting the major contributions Canadian mathematicians continue to make. In this case, there is already plenty of proof available.
Thankfully, there is not an art component to the Fields postdoc application.

Q: What do you get when you give a group of mathematicians complete creative freedom on Halloween?

A: Math pumpkins.

What’s a mathematician’s favourite dessert?

The costume component had a little more range.
Future leaders combine efforts to prepare Canada for the next health emergency at MfPHest (Mathematics for Public Health Festival).

A little lunch and libretto: Fields organized a midday culture hit at the Canadian Opera Company.

Spain’s Ambassador to Canada, Alfredo Martínez Serrano, enters the Institute’s handshake Bermuda Triangle.

We love math so much at Fields that it’s truly nose-blowing.

Sad cactus once sprouted flowers for a few days, but they died.
Venkatesh was awarded the Fields Medal in 2018 “for his synthesis of analytic number theory, homogeneous dynamics, topology and representation theory, which has resolved long-standing problems in areas such as the equidistribution of arithmetic objects.”

True to form, Venkatesh asked to do things at this Symposium a little differently. Rather than a program dedicated only to his work, he preferred an opportunity for speakers from diverse fields to address the influx of new perspectives on the nature of research and of proof. Given the evolving technological landscape we are living in, it was a topic very much of the moment and one that acknowledges the inextricable relationship between research and its context.

The 2022 Fields Medal Symposium took place in hybrid form, inviting participants to chime in online, or come in person to the Fields Institute for the first time since 2019.

For his Public Opening talk, Venkatesh chose to speak about “Glimpses from Entropy’s Lens”. The event was held in person at the Isabel Bader Theatre on the University of Toronto campus. At the door, staff handed attendees a balloon before ushering them to their seats. This unusual prop would make perfect sense at the top of Venkatesh’s talk, when he encouraged the audience to participate in an experiment first posed in an early 19th century letter by British experimental philosopher, John Gough. Gough’s investigations into the properties of natural rubber led to the first description of the heat that gets released when rubber is stretched quickly. He noticed that after the stretched rubber heats up, it contracts, which is the reverse of what normally happens to materials when they’re heated. This experiment later influenced physicist James Joule, who discovered the relationship of heat to mechanical work and for whom the joule unit of energy is named.

This fun, interactive experiment was a great lead-in to Venkatesh’s exploration of entropy, a subject he chose because it interests him personally. Not every mathematician can speak about physics so clearly and find the natural links to their own areas of research. The fact that Venkatesh can pull this off, and that he chose to speak about this topic at a Symposium traditionally designed to honour Fields Medal-winning work, indicates a curious mind that loves to explore the boundaries of its own knowledge. Numerous attendees later commented that they appreciated the opportunity to hear someone of Venkatesh’s level speak on a topic they could follow without advanced mathematics training.
DIGNITARIES
The Honourable Scott Ryan
High Commissioner of Australia
Nalini Joshi
Vice-President of the International Mathematical Union (IMU)

STUDENT NIGHT
We were pleased to host the first Student Night since 2019. This popular, sold-out event offered high school students and undergraduates the opportunity to interact with a Fields medallist and working mathematician.

Venkatesh spent several hours chatting with attendees over pizza, gamely answering questions and offering advice, inspiration and direction.

ORGANIZING COMMITTEE
Kevin Buzzard
Imperial College London
Maia Fraser
University of Ottawa
Michael Harris
Columbia University
Alma Steingart
Columbia University

SCIENTIFIC PROGRAM
SCHEDULE
Monday, October 17, 2023
Opening Remarks
Kumar Murty
The Fields Institute; University of Toronto
Akshay Venkatesh
Institute for Advanced Studies
Michael Harris
Columbia University
Abstract Formalities
Johan Commelin
Albert Ludwigs University of Freiburg
Prospects for AI Systems That Can Form Concepts and Abstractions
Melanie Mitchell
Santa Fe Institute
Towards General and Robust AI at Scale
Irina Rish
Université de Montréal; Mila

“The people always say there is no universal mathematician nowadays because it is too difficult, but [Venkatesh’s mind] can think about anything.” Emmanuel Kowalski, Swiss Federal Institute of Technology Zurich.

THE FIELDS MEDAL SYMPOSIUM
Tuesday, October 18, 2023
What Can the Working Mathematician Expect from Deep Learning?
Geordie Williamson
University of Sydney
Is mathematical interest just a matter of taste?
Timothy Gowers
Collège de France
What makes a proof acceptable?
Andrew Granville
Université de Montréal
How I became seduced by univalent foundations
Emily Riehl
Johns Hopkins University

Wednesday, October 19, 2023
Varieties of Mathematical Understanding
Jeremy Avigad
Carnegie Mellon University
Tacit knowledge and partial automation in mathematics
Rodrigo Ochigame
Leiden University
Closing Remarks
Kumar Murty
The Fields Institute; University of Toronto

The Public Opening was recorded and the full video is available on our YouTube channel.

The Scientific Program was streamed live and also recorded for later viewing on our YouTube channel.
Q: The physics-to-math pipeline can be a natural trajectory, but not everyone makes the full leap. What inspired you to make the transition?

My early research experiences were in experimental physics. One of them was working at the LIGO (Laser Interferometric Gravitational-Wave Observatory) lab at Caltech over a summer. That is when I first got interested in understanding the many theoretical aspects in physics that were relevant to LIGO, such as quantum optics and general relativity. It was this natural curiosity to understand foundational aspects of experimental observations that first got me more interested in mathematics and eventually helped the transition. Though I had to spend quite some time during graduate school catching up with basic undergraduate mathematics, the journey was immensely satisfying. Also, more than anything, it felt like the most natural thing for me to do.

Today, I look at mathematical questions that arise in general relativity, like the theory of gravitation proposed by Einstein. More specifically, I investigate questions concerning the stability and uniqueness of stationary spacetimes. These spacetimes are what could be considered, in some sense, equilibrium solutions to the Einstein equations. So, some natural questions to address are the stability and uniqueness of these solutions. How to precisely characterize the stability/instability and uniqueness for some specific spacetimes is what I spend a lot of time thinking about.

Another aspect of mathematical relativity that I have been interested in more recently is near horizon geometries. A specific case of a Quasi-Einstein (QE) manifold. These can be seen as generalizations of Einstein manifolds, Ricci solitons or smooth metric measure spaces. Broadly, it is about the existence/non-existence of certain kinds of QE manifolds or, in other words, restrictions that get imposed on these manifolds under certain and/or charge for a given mass. It can roughly be thought of as a codimension 2 hypersurface describing a degenerate horizon in spacetime. What I have been investigating along with my collaborators is the classification and uniqueness of near horizon geometries. This problem has a greater connection to the thematic program.

Q: What have you been working on since you came to Toronto?

I recently published a paper about the classification and rigidity of near-horizon geometries. A specific case of a Quasi-Einstein (QE) manifold. These can be seen as generalizations of Einstein manifolds, Ricci solitons or smooth metric measure spaces. Broadly, it is about the existence/non-existence of certain kinds of QE manifolds or, in other words, restrictions that get imposed on these manifolds under certain...
conditions. During my time at Fields, working further on this problem has brought up many other questions and this has since evolved into a bigger research program - “uniqueness of near horizon geometries”. We are in the process of wrapping up work in this direction.

**Q:** Any interesting results?

The results in the paper mentioned above are related to the idea of Bakry-Émery Ricci curvature which has been studied in optimal transport, Ricci flow, and general relativity. A specific case of quasi-Einstein manifolds/near horizon geometries is a static vacuum near-horizon geometry, which is an extreme black hole that admits a hypersurface orthogonal timelike Killing vector field. It was known that when the cosmological constant vanishes, there is rigidity for the static near-horizon geometries i.e., one has only Ricci flat solutions. We investigated this form of rigidity for all signs of the cosmological constant in the paper.

One of the main themes in the thematic program was the non-smooth formulation of general relativity. If one defines black holes using non-smooth concepts, then a question that can be asked is what can one say about the horizon and known results about horizons? What is a degenerate black hole in this setting? In contrast, our results focus on knowing the smooth case better which one should presumably do first.

**Q:** How did Fields help you achieve your research goals?

Most of my work to date has been in the smooth setting of general relativity. It was instructive to know the right questions to be asked in the low regularity/non-smooth setting. This way, I had the opportunity to explore many research ideas I might not have been equipped to do in solitude. All in all, the program was a rich environment for connections and potential collaborations.

**Q:** What’s your experience at Fields been like so far? Highlights?

I’ve been having a great time at Fields so far. It’s enriching to interact with all the visitors and we are able to inform each other about the big picture in each other’s fields. As an added bonus, I’ve also gotten to know the members of the Differential Geometry and Analysis Group in the Department of Mathematics at the University of Toronto. The best part of the workshops was the energy and enthusiasm throughout – members of the organizing and scientific committee stimulated very interesting discussions after the formal talks.

More specifically, my collaborator and postdoc supervisor, Eric Woolgar, was a part of the program and in residence for the entire duration of the program. This was the longest in-person interaction that was possible for us after COVID-19 lockdowns. I’ve also benefited from conversations with Robert McCann over tea time about the non-smooth formulation of general relativity. As I look forward to these interactions, I am quite punctual for tea. This is perhaps also the reason why I have always found enough cookies!

**Q:** What’s something people might be surprised to learn about you?

I would like to become a science journalist some day and record a podcast of science-themed bedtime stories for kids! In each issue, we will spotlight a postdoc researcher and their work.

In each issue, we will spotlight a postdoc researcher and their work.
2023 Fields Medal Symposium

Caucher Birkar
2018 Fields Medallist

The Fields Institute
222 College Street
Toronto, Canada

October 16-20
OpenAI’s large language model (LLM) tool has dominated the media cycle in a way few machine learning applications have managed to achieve. It has singlehandedly expanded our notion of chatbots by mimicking human-like conversations and generating detailed, articulate responses to almost any query on the fly. It can also compose music, code and debug computer software, write poetry and take your third-year biology test. When it hit the market last November, ChatGPT became the fastest-growing product launch in history, reaching 100 million users in two months. For some perspective, it took TikTok, the second-fastest product launch in history, nine months to achieve those numbers.

ChatGPT’s answers are still uneven, with accuracy levels ranging from formidable to unintentionally hilarious. But the speed at which the model is improving itself has convinced many experts we are rapidly approaching artificial general intelligence (AGI), or the point at which machines can learn an intellectual task the same way humans can. This proclamation, coupled with uncertainty over how its capabilities will impact existing social frameworks – from university grading to job requirements – has reinvigorated public debate about the future of artificial intelligence: In March, over 1,000 leaders in tech, academia and politics signed an open letter asking for a pause in large-scale AI experiments, citing fear of potential harm to humanity. Later that month, Italy banned ChatGPT until its privacy concerns were better defined.

As usual, the actual mechanics have gotten lost in the hype. For starters, ChatGPT is not built on a new idea – the fundamental architecture has been around for more than six years – but it is a marvel of engineering with immense power and potential. It’s also a story of betting everything on the right horse. And at the core of it all is, you guessed it, mathematics. For those interested in what is going on under the hood, here’s a human-generated primer on the technology of the moment.
OpenAI and the Toronto connection

Back in 2015, the Toronto Star published a lengthy article about an academic from the University of Toronto named Geoffrey Hinton. The headline suggested his research had “revolutionized” modern artificial intelligence and recalled how he had toiled in obscurity for decades, a marginal and - to the world of computer science - a somewhat unserious figure who was convinced that computer neural networks, which could mimic the brain and therefore “learn” like humans, were the future of artificial intelligence.

The condescension stopped around 2006 when Hinton’s neural nets, rebranded as “deep learning,” began beating every previous AI benchmark. By 2012, Hinton’s lab gained international attention for winning ImageNet, Stanford’s image recognition contest. The lab’s computer vision model shattered records and forced critics to concede that Hinton may have been onto something the whole time. The paper that emerged from the ImageNet contest is widely considered to be a turning point in the current AI boom. Its co-authors were two of Hinton’s grad students: Alex Krizhevsky and Ilya Sutskever.

Sutskever would go on to co-found OpenAI with some of Silicon Valley’s biggest names. As chief scientist, he now oversees the company’s R&D operations and has developed a reputation for pushing hard on passion projects. He began developing the first GPT model in 2018 as an evolution of his own ground-breaking research in natural language processing (NLP), or the area of machine learning that trains a model to recognize and interpret human language. But Sutskever was not the only scientist working on a large-scale NLP project, and OpenAI was considered an “underdog” compared to some of its competitors building similar large language models. So how did OpenAI manage to come out ahead of behemoths like Google and Meta?

The answer is a combination of intuition, luck and sheer doggedness. For the past few years, AI companies have faced huge pressure to make good on the billions poured into their research and start delivering money-making products. This has forced some R&D divisions to put a pin in longer-term research projects with uncertain outcomes and focus instead on products with high commercialization potential. Despite this pressure, Sutskever continued to champion ideas behind the GPT series of models. Like his mentor, Geoffrey Hinton, he was relentless in his belief that large language models would be the right gamble. Now, for the second time in his young career, Sutskever’s contributions have changed the world.
An old idea made new

When the modern AI boom began in 2015, computer vision was poised to become the dominant area of machine learning. Computer vision is a machine's ability to see and interpret the world from digital imagery. Rapid progress in computer vision was aided by the fact that there were billions of parameters of training data already available on the internet, which allowed models to scale quickly and accurately.

At the same time, natural language processing (NLP) models were still struggling with basic problems like negation (i.e., using negative words to change the meaning of a sentence) or synonyms. Because of its limitations, NLP failed to gain as much momentum as other machine learning areas.

That changed with the invention of word vectors. Word vectors are attempts to mathematically represent the meaning of a word by calculating how frequently different words show up next to each other in large chunks of existing text. These correlations are used to train vector embedding models, in which a word (or token) \( t_i \) gets “represented” in a vector space of dimension \( d \) using a mapping function \( f \). These representations were shown to have amazing properties, such as implicitly learning the existence of underlying concepts, with the famous examples of \( f(queen) - f(king) = f(woman) - f(man) \).

Since the vector subtraction yields the same answer, the machine can deduce that there is an underlying concept (gender) that connects the otherwise unrelated words.

While simple at their core, word vectors became an important building block in the evolution of NLP. The next step was to look at sequences of words. But if we wanted to do something this complicated, we needed a new framework – a mathematical way to put the information into the neural network, rather than just working with the text. This new framework was to represent sequences of words (of some length \( n \)) as tensors of dimension \( (n \times d) \).

Sutskever was among the first to develop the intuition that focusing on engineering and scaling up neural networks could solve the area’s technical limitations. In his now famous Sequence-to-Sequence paper, he reinforced the idea that neural networks could learn representations of abstract ideas, like meaning in language, using the right architecture and with enough data. Suddenly, it was possible to experiment with more sophisticated NLP concepts. Machine translation was a natural starting point because the internet already had tons of translated text. These intuitions proved correct: Sutskever’s research ended up contributing to the success of Google Translate, the tool that can now automatically translate text from hundreds of languages with considerable accuracy.

May we have your attention, please

Now that models could interpret sequences of words, it became possible to expand to long, connected sentences in substantial paragraphs. Sutskever proposed using an architecture called LSTM. LSTMs, or Long Short-Term Memory networks, use an idea called “recurrence” to model language. Recurrent networks use memory to link sequences of words together so that, in a

Figure 1: An example of word vectors from Creating Word Embeddings: Coding the Word2Vec Algorithm in Python using Deep Learning by Eligijus Bujokas.
paragraph of text, the output of a sentence depends on the input of the previous sentence. However, this architecture was not computationally scalable and struggled with tracking context over long sequences.

After some iteration, a paper came out in 2017 called Attention is all you need by Ashish Vaswani et al. and it would make the next stage of natural language processing possible. The authors proposed that recurrence can be completely abandoned in favor of focusing on a component called “self-attention.” Unlike recurrence, which links inputs and outputs in a linear sequence, a self-attention module allows all the inputs to interact with each other simultaneously (this would be the “self” part) to figure out what they should pay “attention” to in order to modify an output sequence with the most relevant information. A network built on this concept is called a Transformer network.

Mathematically, the idea behind self-attention is simple, and follows a basic two-step process:

1. \[ z_{\text{raw}}(i, j) = \sum_{k=1}^{n} w_{k, j-1} z_{i-1, k} \]
   where \( z_{i, j} \) is the embedding of the \( i \)\_th token at the \( j \)\_th layer of the Transformer network

2. \[ z_{i, j} = f(z_{\text{raw}}) \]
   where the weighted sum of the tokens is passed through a non-linear tokenwise layer \( f \) (a basic “multilayer perceptron” neural network, the most standard kind)

It turned out that stacking these two operations (above) created a very rich, expressive neural network architecture that proved more computationally efficient and could be scaled up to very large networks.

All this work showed very promising results around machine translation, but something was still missing to take it to the next level.

**BERT has entered the chat**

The missing link, in this case, has a name that sounds like it belongs on Sesame Street. BERT is an acronym for Bidirectional Encoder Representations from Transformers and is a framework to train a Transformer model that can encode text in a very general way. In other words, it enables most tasks in natural language processing, like identifying sentiment, answering questions or locating the names of objects by abstracting from a specific task to realize it’s the same no matter in what context it’s being asked.

As unfortunately named as BERT may be, none of the lead-up to ChatGPT would be possible without it. Before BERT, natural language processing had a bottleneck problem by having to train models with specific datasets for each specific task and on completely different architecture. This was time consuming and limited the ability to perform NLP in a cost-effective way.

BERT established a baseline understanding of language, allowing researchers to pre-train and fine-tune models. It works as a sort of fill-in-the-blanks game by helping an algorithm recognize whether two sentences form a logical sequence, or whether...
Scaling unprecedented heights

Here’s where Sutskever’s intuition about the importance of scale really comes into play. In 2019, OpenAI’s research team published a blog post detailing a phenomenon called Deep Double Descent. This new discovery challenged what scientists know about the bias/variance trade-off, or the notion that there are limits to how complex or large models can get while remaining robust. OpenAI’s post showed that models trained on certain datasets could be scaled indefinitely, even improving the model over time.

After this discovery, researchers started tinkering with the method they used to train a Transformer to “speak,” by choosing a game that had the network guess the next word in a sequence. This new game, combined with scaling language models to an unprecedented capacity, gave rise to what we now call large language models. This discovery was the defining moment when everything came together to make ChatGPT possible.

Bringing everything into alignment

What OpenAI did next was spend three years getting really good at alignment.

Success in alignment, or fine-tuning, can make or break a model. Here’s how it works. Say you want to build a language model to flag certain topics, like recognizing news articles about sandwiches. In previous NLP paradigms, you would have to find thousands of news articles and label them manually before feeding them to the model; this article is about sandwiches, this article is not about sandwiches, etc. After the labelling was complete, you would fire up BERT and use its logical analysis of language to do something called fine-tuning. During the fine-tuning process, you incorporate another model that’s good at predicting the next sentence in a sequence, show it all the data you’ve collected, then change or “tune” it slightly to focus on finding articles that are about sandwiches or not about sandwiches.

Fine-tuning large language models is much different from fine-tuning earlier language models. For starters, you need a lot less data than the previous paradigms. OpenAI invested heavily in finding ways to improve alignment techniques and achieved a new benchmark with GPT-4, their most recent and most powerful ChatGPT model. GPT-4 has blown past benchmarks with its ability to draw out latent logical skills that help the model get better at predicting the next word in a sequence in the way a human would accept as characteristic. For instance, logic, in this case, is how a model learns how to write like Shakespeare. Or like a toddler. Through logic, the model can accurately predict how Shakespeare or a toddler would use language to complete the next sentence, instead of just providing a more generic option. It’s the ability to provide rapid, well-constructed responses in the voice or syntax of the original query that has caused the biggest stir amongst users.
OpenAI may also have some new alignment tricks up their sleeve, which they haven’t yet made public. Any improvements will undoubtedly build on the technical proficiency already exhibited by existing GPT models. But here’s the winning hand: Ultimately, OpenAI came out ahead in the large language model race because Sutskever understood that ChatGPT needed, above all else, to be useful to humans and a machine learning application is only useful if it aligns with human expectations.

**Rev up your engines**

While OpenAI may be credited with the first “best” model, the race has just begun and ChatGPT’s success has spurred competitors to catch up. Google is hot on OpenAI’s heels, as are other scale-ups like Anthropic and Toronto’s Cohere AI. Regardless of which platform produces the world’s best large language model at any given time, it is undeniable that the world is set to change.

An immediate change is in the way we now talk about artificial general intelligence (AGI). Two years ago, anyone who spoke about AGI occurring in our lifetime was treated much like Geoffrey Hinton in the early 2000s. They were dismissed as having their head in the clouds and not taken seriously. Today, it is foolish not to consider that, at this rate, we are far closer to AGI than we realize. In fact, Hinton himself recently resigned from Google so he could freely speak out about his concerns about where AI is heading.

The next phase of ChatGPT discovery demands that we revisit age-old questions about AI safety, AI alignment and how the economy will adapt to this new machine reality. Mathematics has an important role to play in this transition by helping answer fundamental questions like whether aligning an AGI to human goals and ethics is even possible, what the scaling limits of large language model performance are, both in terms of computation and the amount of data available to train these models.

Thankfully, we have not yet outsourced the answer by asking ChatGPT the big, existential questions.

Alik Sokolov is Managing Director, Machine Learning, at the University of Toronto’s RiskLab and Co-Founder/CEO of AI-driven investment start-up, Responsibli.

---

**Figure 4: Deep double descent breaks machine learning expectations** – where a model would be expected to begin performing worse on a hold-out set due to overfitting, the model eventually “rebounds” and once again begins decreasing its out-of-sample loss. A great new mathematical mystery!

Source: Deep double descent from the OpenAI blog (December 5, 2019).
Let's take RSA encryption as an example. This technique uses modular arithmetic to encrypt and decrypt messages. Here's how it works:

Bob wants to send a message $m$ to Alice. The message $m$ is encoded as an integer of a fixed size. Alice chooses two large prime numbers $p, q$ and multiplies them together to get a number $n := pq$. Alice will then choose an encryption key $e$ which is less than $n$, and has no common factors with $n$. Alice will also compute a decryption key $d$, such that for all numbers $x$ between 1 and $m$, $x^{e \cdot d} \equiv x \pmod{n}$. Alice publishes the values $n$ and $d$ as her public key. If Bob wants to encrypt a message $m$ to send to Alice, he computes a ciphertext $c := m^e \pmod{n}$. If Alice wants to access the message, she computes $c^d \pmod{n}$. Notice that $c^d \pmod{n} = (m^e)^d \pmod{n} = m \pmod{n}$.

The key to computing the decryption exponent $d$ is the ability to factor the number $n$ into its prime factors $p, q$. Without knowing these prime factors of $n$, it is considered computationally infeasible to compute the value of $d$. But, since Alice knows the prime factors of $n$, it is easy for her to compute the value of $d$. In principle, the value of $d$ is computable from the knowledge of $e$ and $n$, but it would take a classical computer thousands of years to do the necessary computations to yield the answer. The security of RSA encryption is derived from the computational difficulty of decrypting for anyone other than Alice, who holds the private key.


Cryptography is the practice of securing information to prevent third parties from accessing it. You can think of it more simply as creating a code to ensure private messages don’t get read by anyone who shouldn’t be reading them. Like the time you invented a cipher with your friend in Grade 5 so you could pass notes in class without fear of what would happen if the teacher intercepted. No key to the cipher? Your teacher wasn’t going to be reading anything out loud to the class that day.

On a computational scale, cryptography gets far more complex. It requires a thorough understanding of mathematics, specifically algorithms designed around computational hardness assumptions. In other words, how difficult it would be for a computer to decrypt, i.e., “crack the code” of a message without access to a key.

Any cybersecurity program worth its weight will have a core cryptography module that includes techniques like RSA encryption, and graduates should have a firm grasp of these mathematical principles before they enter the workforce. To create secure systems requires a foundational understanding to anticipate new ways bad actors can subvert security protocols.

**Warning: Steep cliff ahead**

Did you follow the logic in the RSA encryption above? That's good. Unfortunately, things are about to get a lot more complicated: quantum computing threatens to compromise the security of numerous protocols we rely on for the verification of online identity as well as encryption.

Quantum computers are like classical computers in the sense that they are able to perform computations using inputs and outputs of strings of 1s and 0s – or “bits”. Let's say we've got three
bits: \(a\), \(b\) and \(c\). Each can take on the value of 0 or 1. I want to do a computation using \(a\), \(b\) and \(c\) whose outcome depends on their values. A classical computer would have to assign every possible value assignment to \(a\), \(b\) and \(c\) so that every possible value assignment is \(2^{\text{3}}\).

A quantum computer could, instead, form something called a superposition of states in which each of \(a\), \(b\) and \(c\) are able to simultaneously hold the values of 0 and 1. With superposition, the machine can perform certain computations on all eight of these states in a single operation. In some situations, this facilitates a significant computational speed-up that can’t be achieved on a classical computer. For example, this quantum advantage allows us to factor numbers very efficiently, which makes it easier to break security protocols like RSA encryption.

To date, this computational ability remains in the hypothetical realm, but the technological gap is closing and we need to be prepared. This means changes have to come to public key cryptography. Specifically, the so-called “hard” problems that provide the foundations of many online security measures are no longer hard if you have a quantum computer. Anyone with a public key will be able to compute the private key, which defeats the purpose.

This has prompted a rethinking of the mathematical foundations that we use to ensure everything from secure online payments to transactions on the blockchain. Preparing for this presents a massive logistical challenge for both government and private industry as they get ready to update older cryptographic software and hardware with more secure variants before a quantum attack becomes technologically feasible. The organizations preparing for this inevitability will be far better situated when that day comes.

How nature inspired the quantum quest

So how did we get here? Since the 1970s, modern public key cryptography has solved problems related to confidentiality, the integrity of data and the authentication of identity using mathematical schemes called “trapdoor” problems. These are processes that can be performed very efficiently one way, but are extremely difficult to reverse. In every case, the security of the system depends on the difficulty of reversing some process. When a computational trapdoor is tricky enough, it is essentially impossible for someone to break through the encryption without a public key.

Quantum leap

By 1985, British physicist David Deutsch had discovered a rigid formal model of quantum computation, and researchers began developing quantum algorithms which could be implemented on a hypothetical quantum computer.

In 1994, Peter Shor at Bell Labs was successful. Shor’s algorithm would be able to perform a large number of classically hard problems very efficiently and set the stage for a potential industrialization of quantum computers in the future. Notably, Shor’s algorithm was able to factor large integers and compute discrete logarithms over both finite fields and elliptic curves in polynomial time. These are exactly the kinds of trapdoor problems that underpin the security of essentially all modern public key cryptosystems. With Shor’s discovery, we had reached an understanding, in principle, that if a quantum computer were to be built, these cryptosystems would instantly collapse, creating a security catastrophe.

By the early 2010s, a few quantum computers started to appear but they were very limited in scope. None of these computers could implement any given quantum algorithm the way a basic laptop can run any software program. Instead, these machines were purpose-built to perform very specific computations.

And so it remains to this day. No one has successfully implemented Shor’s algorithm in a way that could break universal encryption, and the timeline for this scary moment remains unknown. The first actor to successfully achieve this feat would have unprecedented powers of surveillance over the rest of the world. But just because we haven’t seen it happen yet doesn’t mean this surveillance isn’t already underway. And like Y2K, disaster can only be averted if we proactively update all of our systems. If a large organization had reason to believe they could...
build a quantum computer in the near future, they could already begin intercepting secure communications with the intent to decrypt them down the road when they have the right tools. A government typically classifies documents for about 30 years, after which they figure the information they contain is no longer harmful. That means any government relying on encryption to keep secrets should be asking themselves not whether a quantum computer exists, but whether one could exist in the hands of an adversary within 30 years.

**Ensuring Canada is able to safely keep passing ‘notes’ in class**

Now begins the very difficult task of implementing these new algorithms and integrating them into our electronic infrastructure. Unfortunately, the scope of this task isn’t completely clear, which leaves us vulnerable in the interim. The Canadian Forum for Digital Infrastructure Resilience (CFDIR), a public-private collaborative body dedicated to ensuring the security and resilience of critical digital assets in Canada, has convened a Quantum Readiness Working Group (QRWG) to study solutions and strategies to respond to this problem in a timely and effective manner. In July 2021, they published a document outlining best practices and guidelines for organizations looking to migrate to quantum secure infrastructure. To date, nothing more substantive has been distributed, but it’s a start.

The QRWG-recommendations require that Canadian companies and governmental agencies foster internal teams to understand the threats posed by quantum computing, and to catalog IT assets that need to be updated or replaced. As usual, there is a communications problem: many organizations may not even be aware of the countless ways their IT infrastructure relies on quantum-insecure encryption, and the process of identifying and classifying these assets alone could take years. That’s provided there are even enough skilled professionals to scale that mountain. Canada already faces a substantial talent gap in the cybersecurity industry, with estimates of a labour deficit of 25,000 jobs as of 2022. This number will likely grow as more Canadian companies begin to develop their quantum migration strategies, which will lead to an explosion of jobs.

Fields sees this as an opportunity for talented young Canadians with the technical capability to understand the intricacies of the quantum threats to cryptography and the technical solutions required to mitigate them. At Cyber Connexion, our curriculum is designed to help prepare for a post-quantum future. We help place our graduates at forward-thinking partner companies, closing the talent gap one expert at a time.

Interested in fast-tracking to an exciting new career in cybersecurity? Visit our website to learn more: cyberconnexion.ca.

Aaron Crighton is Cyber Connexion’s Academic Liaison. He completed his PhD in mathematics at McMaster University.
Vanessa Vakharia wants to do away with the constricting labels we give to ‘success’ and ‘failure’ in the K-12 classroom.

How many times have you set out to achieve something and “failed,” according to the traditional definition? Would you still label that as failure in the pejorative sense?

Too often, failure is wielded as a punishment in the classroom. This approach imbibes students with a fear of consequence that can shut down the resilience they need to develop to push through struggle. Part of the problem is that, in many cases, there are consequences and they are unequally distributed. For every student who feels supported and has the resources to improve their academic performance, there are dozens who slip through the cracks and never recover momentum. This is a different type of failure; one that teaches young people that their efforts may not amount to anything, so there is no point in even trying.

As a math educator and advocate, but also a student who flunked Grade 11 math twice, I’ve been on both sides of the equation. By luck and privilege, I landed in the Grade 12 classroom of a teacher who encouraged her students to do away with terms like “math person” and bring our whole selves to the subject. Her approach changed my life. Today, I run a boutique math tutoring centre in Toronto that has helped hundreds of students improve their grades and foster a love of mathematics. If I hadn’t ended up with that specific teacher, I would have missed out on a career path that has brought me great meaning and fulfillment. But neither luck nor privilege should be the deciding factor when we have the tools and research to improve educational outcomes more broadly.

Math class is somewhat of a lightning rod for this principle. In theory, it has the potential to teach students some of the most important skills: how to take risks necessary to solve the most complex problems, and how to be comfortable with failure as part of that process. When we discourage failure and focus only on correct answers or narrow-minded views of mathematical ability, we are not only deterring students from pursuing mathematics, but also from developing the grit needed to pursue any goal.

Embracing a growth mindset

Research from Jo Boaler et al (In the paper, From Performance to Learning: Assessing to Encourage Growth Mindsets, Jo Boaler et al) has shown that students who achieve the most in mathematics are always pushing to the edge of their understanding. They make mistakes, fail, struggle, but ultimately learn from the experience. Stanford professor Carol Dweck coined the term “growth mindset” to describe this phenomenon. Unlike a fixed mindset, where students believe in a static idea of their intelligence and, as a result, tend to shy away from struggle, students with a growth mindset are convinced of their ability to keep learning and are more likely to embrace challenge. It is the second group of students that consistently achieves better outcomes.

Dweck’s research has influenced many educators, including JUMP Math founder, John Mighton; yet, there is still some resistance to this approach. In Building Thinking Classrooms in Mathematics, Peter Liljedahl argues that the mathematics curriculum in many schools teaches students to mimic instead of think. Exercises are set up to provide students with algorithms and tricks, then have them follow a series of predefined steps. When
students miss a step or do not end up with the correct answer, we penalize them. If they do end up with the answer we are looking for, but do not arrive at it in the way we ask them to, we penalize them. What does this teach students? It teaches them to operate within the confines of a step-based process instead of how to think critically about problems and explore their curiosity. It teaches them that unconventional thinking is frowned upon and that taking risks in order to solve problems creatively leads to a big red “X”.

There is so much to lose in this approach. Today’s greatest problems – from climate change and pandemics to economic instability and racism – require solutions that extend far beyond algorithms and rule-following. We need people who can think creatively and who aren’t afraid to try something new. A huge part of fostering those environments is to embrace the empowering role of failure in our math classrooms.

Applying these lessons to the classroom

I meet so many dedicated, passionate math educators through my work. One thing they have in common is a desire to find new ways to help students overcome their fear of failure and embrace challenge. Here are three methods I use for integrating “failure” into math curriculum:

- Re-examine how we look at binaries like “right” and “wrong” or “good” and “bad” in math class by focusing on the journey instead of the destination.

By honing in on process, students are likely to feel more comfortable taking the risks needed to come up with a solution. Make sure that when you’re critiquing student work that you always comment on the process as well as the result. Open Middle Problems (openmiddle.com) are a great way to get students familiar with creative approaches to risk-taking necessary to solve unfamiliar math problems. In an open middle problem, students all start at the same point, and the goal is for them to arrive at a particular end solution, but what they do in the middle is up to them. The diversity of thought that results from this method is a great way to start the discussion about valuing and respecting different ways of knowing. Failure in getting the right answer is balanced out by the success of learning something new or gaining a new perspective.

- Revisit your assessment practices.

Are you truly encouraging students to learn from their mistakes? Liljedahl recommends an outcomes-based grading practice as opposed to an events-based grading practice. Involve students in the creation of rubrics so they understand how to learn and grow from assessments, as opposed to viewing them as a fixed marker of where they stand in your classroom. Each rubric section should have actionable steps that help students move from one section to the next. This helps them see how growth and learning line up with their final grade.

- Familiarize yourself with the science of Dweck’s growth mindset and brain-based learning, so that you can convincingly approach your classroom with the belief that failure and mistakes are not absolutes but opportunities for students to grow, learn and develop the grit necessary to solve problems. Talk to your students about growth mindset, explain the neuroscience behind it, make sure everyone in the room knows that failure is not an absolute but a stepping stone on our path to discovery.

Vanessa Vakharia is a dedicated teacher, published author and leading expert in the field of youth engagement in education. She runs The Math Guru, a math and science tutoring centre, hosts a popular podcast and is a frequent speaker at math education conferences. Vakharia is particularly passionate about engaging young women in traditionally male-dominated STEM fields and has presented her findings internationally in an interactive and accessible workshop for young people, academics and educators.
It’s been a busy semester for the Fields Academy Ask a Mathematician (AAM) program with many of our visits focusing on the exciting, ever-evolving world of cyber technologies. Since this issue of Fields Notes focuses on this fascinating and important field, we thought it might be fun to highlight some of the related topics our elementary students have been learning about during their visits.

Aaron Chow, Director, Cloud Security Engineering Practice & Principal Cryptographer at Scotiabank has been teaching students all about cybersecurity and cryptography. He starts by taking his classes on a journey through the historical roots of cryptography before delving into some modular arithmetic and the foundations of RSA encryption, which is used to secure many of our modern communications from nefarious forces. His presentations start with Caesar ciphers, where students are shown how messages can be secured by simply shifting letters of the alphabet, and how very easy these types of messages are to break – especially with modern computers. Finally, he describes how properties of prime numbers discovered hundreds of years ago – well before the thought of modern computers – and modular arithmetic can help us today to secure our most sensitive information.

Daniel Johnston, a postdoctoral fellow at the University of Toronto and soon-to-be professor at Purdue University, focuses on how we can use error-correcting codes to send complex messages across great distances, where data often gets lost along the way, and still be able to construct the correct message at the other end. Students get a chance to convert ASCII text – what we write into a computer – into binary (a series of 0’s and 1’s that the computer can read) and then repeat the message in such a way that, even if errors occur, the final message can still be reconstructed into something humans can read.

Finally, we have Mike Zabroki from York University who introduces students to the world of cyber currency. Classes learn about ledgers, coin-mining (and the huge amounts of energy it requires, with the connected environmental impacts), and how people's funds are verified and secured, all while earning “Z-coins” for their responses.

These talks are designed to help students understand the complex world of cybertechnologies and to be able to think critically about many of the things they use every day. They’re also an engaging entry point into numeracy.

Here’s why it’s working

• Firstly, all of the topics we cover have their foundations in number theory. What’s fascinating about number theory is that many of the principles come from pure curiosity-driven inquiry, and sometimes it takes hundreds of years to find a use for them.
Modern cryptography is one such example: the unique factorization of all numbers into prime factors and the extreme difficulty of finding the factors of extremely large numbers is the logic upon which all modern cryptography is built. We can also relate this to the work of James Arthur and the Langlands Program, which is a pinnacle of “math for math’s sake”, but who knows where his intuitions could someday lead us. Teaching students that their curiosity can lead them to important new discoveries is a critical building block for resilience.

• Secondly, the students learn to think critically about information presented to them and to question what they are being told. In the case of cryptocurrency, students are encouraged to consider the validity of such currencies and to compare them to more traditional banking systems. As they will inevitably interact with AI and machine-based learning, it’s important to create a foundation of healthy skepticism about how these technologies are being used.

• Finally, it encourages students to look at how we can use cyber technologies in a multitude of ways. In our error-correcting code workshop, students are asked to imagine a mining colony on Ganymede, one of Jupiter’s moons. The miners send a code back to earth every day letting them know if everything is ok (represented by a ‘1’) or there is danger and they need rescuing (represented by a ‘0’). Given the seriousness of sending a false message, they explore how triplicating the code can greatly reduce the chance that the wrong message gets received due to a random passing solar flare or other celestial interference. Sending secure messages is a critical part of life today and will only become more integral to daily functioning in the future. This demands the safe and accurate transmission of messages, particularly in light of quantum computers.

We are so excited to bring these AAM programs to elementary students and show them how accessible the worlds of number theory and cybersecurity can be, but most importantly how much fun they are to explore.

Want to try your hand at some cybersecurity and error correcting code? Check out http://fieldsacademy.ca/fn-spring-2023 for some interactive activities.

FAREWELL TO THE
Math Knowledge Network
Reflections on six-year adventure

Since 2016, the Mathematics Knowledge Network (MKN) has worked to bring together educators, researchers, professional organizations and community partners interested in mathematics education in Ontario. Its mandate is to mobilize research evidence, connect research and professional communities and contribute to the Ministry of Education’s mathematics goals and priorities.

The MKN had four communities of practice: Mathematics Leadership, Critical Transitions, Indigenous Knowledge and Computational Modelling (Thinking). Each community worked to increase understanding and sharing of evidence-informed practices, improve attitudes towards mathematics, and enhance learning and participation opportunities for all students. The MKN also addressed emergent needs in the education system, such as support for teachers and administrators during the pandemic and the enactment of new mathematics curricula.

Special thanks to the Ministry of Education and the Fields Institute for their support, and to all our partner organizations. We are also grateful to everyone who dedicated their time, expertise and passion, including George Gadanidis (Western) and Donna Kotsopoulos (Western) for their leadership, Melanie Langemeyer and Arielle Figov as MKN coordinators and our CoP’s leads. We are confident that the connections within our network will remain strong and that the legacy of the MKN will provide a firm base for mathematics education in the years to come.

Chantal Buteau and Dragana Martinovic were co-directors of the Math Knowledge Network.
FIELDS OF DREAMS
Postdoctoral fellow Therese Landry shares how her experience at the Fields Institute has inspired her to blaze a trail for underrepresented groups in mathematics

Quick stats
• Postdoctoral Fellow at the Fields Institute from July to December 2022
• Now a Visiting Assistant Professor at University of California (UC) Santa Barbara
• First-generation Filipina-American

Therese Landry started on her path to becoming a mathematician when her son was two years old. She completed her PhD in mathematics at UC Riverside in January 2022 and a few short months later, joined the Mathematical Sciences Research Institute (MSRI) in Berkeley, California as a postdoctoral fellow. She was first introduced to the Fields Institute when she attended a Quantum Dynamics workshop as a graduate student and the experience inspired her to return.

During her postdoctoral fellowship at Fields last year, Landry attended the largest multidisciplinary and multicultural STEM diversity conference in the United States – the National Diversity in STEM Conference (NDiSTEM). Hosted by the Society for Advancement of Chicanos/Hispanics & Native Americans in STEM (SACNAS), the conference serves to equip, empower and energize participants for their academic and professional paths in STEM. Along with this was the Modern Math Workshop, which aims to encourage undergraduates from underrepresented groups to pursue careers in the mathematical sciences.

Landry shared her experience being a first-time speaker at the event, her roundabout path to becoming a mathematician and the importance of providing equitable opportunities for all members of the mathematics community.

How did you get involved in SACNAS? What was the draw for you as a mathematician?
Being a mathematician is my second career. Before this, I spent nearly a decade as a high school mathematics teacher in inner-city Los Angeles. The first step in my journey to becoming a mathematician was receiving my masters degree in Mathematics at San Francisco State University. MSRI is located just across the Bay, so it was especially meaningful to get to have my first postdoctoral position there.

What was the overall experience of attending the SACNAS conference?
Most often at math conferences, sharing research results is the main purpose for delivering a talk. I recognized at the Modern Math Workshop that “who-am-I” stories are key and can be the foundation of research. SACNAS and the NDiSTEM Conference are places where a person’s mathematical journey matters as much as their research results. Mathematics is hard. NDiSTEM helped me see how important it is to carve out spaces for communities like SACNAS, which support people from underrepresented groups as they find the motivation and strength to persist in STEM pathways. Mathematicians from underrepresented groups often have nontraditional pathways to getting established in the profession. Having ample opportunity to meet, connect over and learn
about one another’s experiences was empowering. NDiSTEM was a terrific chance to make new friends, diversify my research network and gain new ideas for professional growth and self-advocacy.

**What was your talk about?**

My talk was entitled “Developments in Noncommutative Fractal Geometry.” As a noncommutative fractal geometer, I look for new expressions of the geometry of a fractal through the lens of noncommutative geometry. At the quantum scale, the wave function of a particle, but not its path in space, can be studied. Riemannian methods often rely on smooth paths to encode the geometry of a space. Noncommutative geometry generalizes analysis on manifolds by replacing this requirement with operator algebraic data. These same “point-free” techniques can also be used to study the geometry of classically pathological spaces like fractals. By expanding the formalism of fractal geometry to include the mathematical language of quantum theory, developments in noncommutative fractal geometry give both mathematicians and physicists the tools to gain insights about quantum behaviors in solids and any new materials made possible by these phenomena.

I know from personal experience that applying for a Postdoctoral Fellowship program is not an easy feat. I discussed submitting an application for a MSRI Postdoctoral Fellowship, and how spending time at another MSRI Graduate Summer School, along with various acts of self-advocacy reinforced by efforts of UC Riverside faculty, helped to strengthen my candidacy. I shared why my fellowships at MSRI and Fields were instrumental in my path to UC Santa Barbara, and the ideas I had gained for new directions in noncommutative fractal geometry as a result of being a Fields Postdoctoral Fellow.

**Do you feel conferences like this are helping improve underrepresentation in math?**

I was a Fields postdoctoral fellow when I gave my talk at NDiSTEM, and I felt a responsibility and privilege in being able to show members of underrepresented groups that someone like them with a nontraditional academic background can also be a Fields postdoc. I believe it’s important to have a growth mindset towards professional goals, especially in the mathematics community. Events like NDiSTEM give participants a chance to hear other mathematicians’ stories and find lessons for their own professional growth. Investing in such initiatives is a powerful way to broaden the participation of underrepresented groups in mathematics.

**What more, from your perspective, can institutions do to close the gap?**

Institutions can further initiate change by helping mathematicians from majority groups explore the role allyship plays in ED&I efforts. Last year, I co-organized a professional development panel on this topic for the Spring 2022 MSRI Postdoctoral Fellows. The discussion focused on how mathematicians at any career level can create a more inclusive atmosphere in our usual professional spaces. Setting aside resources for such discussions and encouraging involvement of mathematicians from majority groups and creating informed allies is an investment from which all mathematicians can benefit.

**Did your experience at Fields provide the support required for both your research and your experience as a working researcher?**

Absolutely. Being a postdoc at Fields gave me the time, space and resources to develop new research directions and contacts. In my last month at the Institute, I submitted a paper resulting from my first collaboration as a postdoc. It was recently accepted for publication in the *Journal of Noncommutative Geometry*. Because of the connections I made at Fields, I’ve had opportunities to give talks on this project, including at the upcoming Canadian Operator Algebras Symposium where I will be a plenary speaker. The Thematic Program introduced me to ideas in optimal transport, and I am now looking into possible projects involving connections between operator algebras and optimal transport.

**Any plans to come back and visit?**

Yes! I successfully applied to be a Long-Term Visitor of Fields Institute Thematic Program on Operator Algebras and Applications, which will be taking place July 1-December 31 later this year.
CONGRATULATIONS TO OUR 2023 AWARD RECIPIENTS

Christian Genest (McGill University) becomes the first statistician to win the CRM-Fields-PIMS Prize while Lynda Colgan (Queen’s University) receives the 2023 Margaret Sinclair Memorial Award

2023 CRM-Fields-PIMS Prize: Christian Genest (McGill University)

The Centre de recherches mathématiques (CRM), the Fields Institute and the Pacific Institute for the Mathematical Sciences (PIMS) were pleased to announce that Professor Christian Genest of McGill University has been awarded the 2023 CRM-Fields-PIMS Prize.

Genest is one of the leading statisticians in Canada, whose work has had dual impact on both theory and real-world applications. He is best known for his contributions to multivariate analysis and was a pioneer in the expansive use of copula models in science. Together with a few close collaborators, he combined nonparametric methods and the asymptotic theory of empirical processes to design a broad array of rank-based inference tools for building, selecting, fitting, and validating stochastic models within this class. Additionally, Genest has contributed to group decision making, prioritization techniques, multivariate extreme-value theory and, most recently, to space-time modeling of rare events in environmental science.

“Christian Genest is the whole package,” said the awards committee. “He has contributed fundamental and pioneering work in a wide range of problems focused on statistical theory. His work on copulas, in particular, has had significant impact on our understanding of the risks of rare and catastrophic events. Moreover, he is a prolific and successful advisor and multiple-time winner of best teacher award in the Faculty of Science and Engineering at Université Laval.”

Genest is a true team worker, quick to point out that his success is a direct result of having the right people around him, from his collaborators to his graduate students and entire family. In this vein, he made it clear that this award is the result of a joint effort and should be viewed as such.

“Research is a complex, long-term venture; it is increasingly difficult to get anything done alone. I like to motivate people and I was lucky to be able to build a team around me and draw expertise from those I’ve collaborated with for many years,” he said. “But our work is also part of a larger scientific agenda to which many others are contributing. To me, this award is mostly the recognition of the importance of our field and the impact of our contributions.”

Genest delivered the CRM-Fields-PIMS Prize Lecture at the Fields Institute on April 20, 2023.
2023 Margaret Sinclair Memorial Award Recognizing Excellence and Innovation in Mathematics Education – Lynda Colgan (Queen’s University)

Lynda Colgan knew Margaret Sinclair from their time at the University of Toronto. The two Ph.D. students shared a supervisor and, post-graduation, kept abreast of each other’s careers as math educators. So, it was a full circle moment when Colgan learned she had received the 2023 Margaret Sinclair Memorial Award Recognizing Innovation and Excellence in Mathematics Education.

“There have been some other nice things that have happened along the way but this is a very important one for deeply personal and professional reasons,” she said from her home in Kingston, where she is Professor Emerita at the Faculty of Education at Queen’s University.

“Other nice things” could refer to any number of the awards, honours and professional distinctions Colgan has accrued over her career. The list is as long as it is varied, but they all take root in her mission to make math more intuitive for children by “seeing and doing through the eyes of a child” and by engaging parents in “Family Math” activities that can reshape negative attitudes.

“Lynda Colgan has devoted her career in education to designing projects and outreach activities, changing the way people see the relevance of mathematics, and making this once-intimidating subject into a field of wonder. She is ensuring Canada knows that mathematics is important, accessible and available to all learners — young and old — and fun!” the committee wrote.

She was also singled out for the success of her outreach work, which the committee tied to her close and empathetic association with students and teachers at many different levels. This quality gives her an unusual capacity to judge what is important and what is apt to be effective.

Teaching is a calling and there is no doubt that Colgan was born to teach. What distinguishes her among educators is her equal passion for the subject matter. She is as much a mathematician as she is a teacher, a “double calling” of sorts that has inspired her to branch out from the classroom and find as many different avenues to share her life’s work.

These avenues have included everything from collaborating on core mathematics curriculum for the province to newspaper columns, television shows, interactive apps, books and papers in noted journals, and countless community efforts to engage parents and students. Two of the shows she helped create, Prime Radicals and Mathxplosion aired on TVO and she wrote an award-winning children’s book, “Mathemagic!”, that sits in many classrooms.

More recently, Colgan has taken the helm as the Executive Director, Education and Development at Science Rendezvous, a non-for-profit dedicated to bringing research and STEM experiences to the public in engaging and interactive ways.

Colgan acknowledges that her “extra-curricular” activities were not always understood in academic circles, another reason receiving the Margaret Sinclair Award is particularly special. “To know that those efforts in bringing creativity and accessibility to mathematics are valued by my peers is incredibly validating,” she said. “That was part of my joy when I got news of the award – that finally someone understood that this work had value and has a place in the total spectrum of what we do as mathematician and as math educators.”

Colgan will deliver the 2023 Margaret Sinclair Memorial Award Lecture at the September 2023 MathEd Forum.
PARTNERS AND SPONSORS

The Fields Institute gratefully acknowledges all of its partners and sponsors for their support and contributions to the Institute’s activities.

Government Support

The Fields Institute holds a Natural Sciences and Engineering Research Council (NSERC) grant through the Discovery Institute Support (DIS) program as well as a grant from the Ontario Ministry Ontario Ministry of Colleges and Universities (OMCU). We also receive support from the National Science Foundation (NSF) for the participation of US-based researchers, especially women and other under-represented groups, in our programs.

Principal Sponsoring Universities

Our Principal Sponsoring Universities (PSU) form a network of world-class mathematicians and researchers that come together at Fields to innovate, collaborate and learn. In return for their support, PSUs receive post-doctoral funding, priority registration for selected events, and more.

Principal Sponsoring Institutions

Our Principal Sponsoring Institutions (PSI) collaborate with Fields to advance mathematical sciences and their application to solving challenges in health, energy, connectivity, and advanced manufacturing.
Thanks to the support of

SIMONS FOUNDATION

ELSEVIER

Affiliate Universities

Our Affiliate Universities help expand the Institute’s reach beyond Ontario and internationally. Affiliate Universities enjoy a special relationship with the Fields Institute.

Corporate Partners

Scotiabank
CANNEX
WATERFRONT INTERNATIONAL
MapleSoft

Partners

Our partners collaborate with The Fields Institute to organize joint programs of mutual benefit to our communities.