

Tushant Mittal

tushant@iitk.ac.in • iitk.ac.in/~tushant

EDUCATION	Indian Institute of Technology Kanpur , Uttar Pradesh, India	Jul 2014 – Present
	▪ B.Tech. in Computer Science and Engineering, 9.2/10.0	
	FIITJEE , Hyderabad, Telangana, India	May 2014
	▪ Board of Intermediate Education, 96.9%	
	Bharatiya Vidya Bhavan's Public School , Hyderabad, Telangana, India	Apr 2012
	▪ Central Board of Secondary Education (CBSE), 10.0/10.0	
RESEARCH INTERESTS	▪ Cryptography ▪ Computational Complexity ▪ Computational Number Theory and Algebra	
PREPRINTS	<i>The Mahler measure for arbitrary tori</i> , with Prof. Matilde Lalin	arXiv Link
RESEARCH EXPERIENCE	Algebraic Independence	Aug 2017 – Dec 2017
	<i>Under Prof. Nitin Saxena, IIT Kanpur</i>	Report
	▪ Studied the computational problem of testing algebraic independence of a set of multivariate polynomials over fields of small characteristic. ▪ Proved a new criterion which relates dependence of polynomials with ideal membership of a non trivial linear combination of their shifted polynomials. ▪ Also explored a new method of dimension reduction to univariates.	
	Mahler Measure	May 2017 – Jul 2017
	<i>Under Prof. Matilde Lalin, Université de Montréal</i>	arXiv
	▪ Studied the Mahler measure of a particular polynomial and the elliptic curve given by its Weierstrass form. ▪ Proved Boyd's Conjecture which was a relation between their Mahler measures and L-function values. ▪ Generalized the relation to a variation of Mahler measure where the defining integral is performed over a more general torus instead of the unit torus. ▪ Work submitted to Research in Number Theory, Springer and is currently under review.	
	Algebraic Geometry	May 2016 – Jul 2016
	<i>Under Prof. Kapil Paranjape, IISER Mohali</i>	Report
	▪ Learned commutative algebra and covered the basics of algebraic geometry. ▪ Explored different aspects of algebraic geometry such as classical, computational, enumerative and projective algebraic geometry and also learnt about Gröbner basis, Schläfli's Double Six. ▪ Rediscovered Kleiman and Laksov's elementary proof of Grassmannian is a projective variety using linear algebra and algebraic geometry which is more accessible than the traditional proofs.	
PROJECTS	Categorical Complexity	Sep 2017 – Dec 2017
	<i>Course Project for Category Theory, taken by Prof. Amit Kuber</i>	Report
	▪ Read and presented the paper Categorical Complexity by Saugata Basu, Umut Isik. ▪ The paper attempts to unify the various models of complexity by defining the notion of complexity of categorical objects like functors and diagrams	
	Adversarial ML	Aug 2017 – Nov 2017
	<i>Course Project for Machine Learning, taken by Prof. Purushottam Kar</i>	Report
	▪ Studied and implemented the method of crafting adversarial inputs, specifically for Google's Inception V3 CNN	
	Cryptanalysis	Jan 2017 – Apr 2017
	<i>Course Project for Modern Cryptology, taken by Prof. Manindra Agrawal</i>	
	▪ Designed and coded differential cryptanalysis attacks for various encryption schemes such as a 6 round DES, RSA with small public exponent using Coppersmith algorithm, 4 round AES	
	C++-Compiler	Jan 2017 – Apr 2017
	<i>Course Project for Compiler Design, taken by Prof. Amey Karkare</i>	
	▪ Implemented an end-to-end compiler for C++, written in Python	

Course Project for Operating Systems, taken by Prof. Mainak Chaudhuri

- Implemented various system calls, scheduling algorithms and comparatively evaluated their performance

**SELECTED
TALKS**

Algebraic Independence - I,II

Series of two talks given in SIGTACS, IITK

Oct 2017

[Slides](#)

Gröbner Basis

Course Project for Computational Number Theory and Algebra, taken by Prof. Nitin Saxena

Apr 2017

[Slides](#)

Democracy's Impossible - Arrow's Theorem

Talk given in Science Coffeehouse, IITK

Mar 2016

Information Theory

Course Project for Discrete Mathematics, taken by Prof. Rajat Mittal

Nov 2015

[Report](#)

Cutting a Cake - Monsky's Theorem

Talk given in Science Coffeehouse, IITK

Oct 2015

Sperner's Lemma

2nd prize in the intra-college SciTalk competition

Aug 2015

**ACADEMIC
ACHIEVEMENTS**

- **MITACS Globalink Research Internship** 2017
- **Summer Research Fellowship Programme, Indian Academy of Science** 2016
- **Joint Entrance Examination (JEE Advanced)** , Rank 186 / 1,20,000 2014
- **KVPY National Fellowship, DST, Government of India** 2014

**GRADUATE
COURSES**

- Approximation Algorithms *
- Algorithmic Game Theory *
- Computational Complexity
- Computational Number Theory and Algebra
- Sheaves and Topos Theory *
- Category Theory
- Modern Cryptology
- Randomized Algorithms
- Elliptic Curves and Applications

* - Courses to be taken next semester

**TEACHING
EXPERIENCE**

Tutor - Fundamentals of Computing

- Selected as one among 12 tutors for the introductory programming course with 450 students.
- Taught weekly tutorial lectures, supervised the lab practice sessions and graded students .
- Also had the responsibility of designing questions for lab assignments, midterm and endterm exams.

Volunteer Teacher, Shiksha Sopan, IITK

- Volunteered with Shiksha Sopan, an NGO aimed at providing education to economically weaker section of the society.
- Taught mathematics at a primary government school in the nearby Bara Sirohi village.

**EXTRA
CURRICULAR**

Quizzing

- An avid quizzier, I have participated and won at many intra-college quizzes and inter-school competitions.
- Managed the Quiz Club, IITK's affairs as the Secretary in 2015-16 and as the Coordinator in 2016-17.

Science Talks

- I also love giving/attending science talks and won the **second prize** in the Intra-College SciTalk Competition.
- Chosen as the **Leader**, Science Coffeehouse, IITK a hobby group where discussions and talks are held on a wide number of scientific topics, for the academic year 2016-17

Volunteer - FSTTCS'17

- Will be attending and also volunteering at *Foundations of Software Technology and Theoretical Computer Science* (FSTTCS), 2017 to be held at IIT Kanpur

**TECHNICAL
SKILLS**

- Languages : Sage, Mathematica, C/C++, Python, Octave, Bash, Verilog
- Web Development : HTML/CSS, PHP, SQL, Django,
- Utilities : \LaTeX , GNUPlot, Git, SQLite