Ali Zare – Portfolio

Ali Zare – Academic & Technical Portfolio

Welcome! I'm **Ali Zare**, an undergraduate student of mathematics at the University of Tehran, driven by a passion for rigorous problem solving, open-source technologies, and the mathematical foundations of cryptography. This portfolio expands on my resume with a deeper look into my academic background and technical projects, curated for those interested in mathematical depth, applied number theory, and Linux system internals.

Contents

Detailed Mathematical Coursework

Here are the primary texts and topics from my mathematics courses at University of Tehran:

- **Algebra-I**
  Primary Text: Abstract Algebra by David S. Dummit & Richard M. Foote

  Topics: Group and Ring Theory, Homomorphisms and Isomorphisms, Cyclic Groups, Lagrange's Theorem, Direct Products

- **Algebra-II**

- *Primary Texts: Abstract Algebra* by David S. Dummit & Richard M. Foote, *Field and Galois Theory* by Patrick Morandi
- *Topics:* Galois theory, Finite field extensions, Hilbert Basis Theorem, PID/UFD/ED, Normal/Separable Extensions

- **Mathematical Analysis-I**
  Primary Texts: Principles of Mathematical Analysis by Rudin, *Mathematical Analysis* by Apostol

  Topics: Sequences, Series, Continuity, Compactness, Connectedness, Real/Complex number systems

- **Mathematical Analysis-II**
  Primary Texts: Principles of Mathematical Analysis by Rudin, *Mathematical Analysis* by Apostol

  Topics: Differentiation, Taylor's Theorem, Riemann-Stieltjes Integral, Uniform Convergence, Gamma Function

- **Elementary Algebraic Geometry**
  Primary Text: Ideals, Varieties, and Algorithms by David Cox & John Little & John B. Little & DONAL OSHEA

  Topics: Affine Varieties, Gröbner Bases, Nullstellensatz, Buchberger Algorithm

- **General Topology**
  Primary Text: Topology: A First Course by Munkres

  Topics: Topological spaces, Continuity, Connectedness, Compactness, Tychonoff Theorem

- **Advanced Calculus**
  Primary Text: Calculus on Manifolds by Spivak

  Topics: Multivariable Calculus, Differential Forms, Stoke's Theorem

- **Elementary Number Theory**
  Primary Text: Elementary Number Theory and Its Applications by Rosen

  Topics: RSA, Diffie-Hellman, Chinese Remainder Theorem, Quadratic Reciprocity, Continued Fractions

- **Graph Theory**
  Primary Texts: Introduction to Graph Theory by West, *A First Course in Graph Theory* by Gary Chartrand & Ping Zhang

  Topics: MST, Trees, Bridges, Eulerian and Hamiltonian Graphs

- **Complex Functions**
  Primary Text: Functions of One Complex Variable I by John B. Conway

  Topics: Mobius Transformation, Cauchy's Theorem, Analyticity, Riemann-Stieltjes Integration

- **Fundamentals of Mathematics**
  Primary Text: Set Theory: A First Course by Daniel W. Cunningham

  Topics: ZFC, Cardinality, Axiom of Choice, Zorn's Lemma

- **Basics of Combinatorics**
  Primary Text: Discrete Mathematics and Its Applications by Kenneth H. Rosen

  Topics: Induction, Pigeonhole Principle, Generating Functions

- **Linear Optimization-I**
  Primary Text: Linear Programming and Network Flows by Mokhtar S. Bazaraa & John J. Jarvis & Hanif D. Sherali

  Topics: Simplex Method, Duality, KKT Conditions, Convex Sets

- **Probability-I**
  Primary Text: A First Course in Probability by Sheldon M. Ross

  Topics: Conditional Probability, Expectation, Random Variables, Chebyshev's Inequality

- **Numerical Analysis**
  Primary Texts: Numerical Linear Algebra and Applications by Biswa Nath Datta, *Numerical Analysis* by David Ronald Kincaid & Elliot Ward Cheney

  Topics: LU/SVD Decompositions, Floating-Point Arithmetic, Numerical PDEs

- **Linear Algebra**
  Primary Texts: Linear Algebra by Stephen H. Friedberg & Arnold J. Insel & Lawrence E. Spence , Terence Tao's Lecture Notes

  Topics: Vector Spaces, Eigenvalues, Gram-Schmidt, Diagonalization

- **Calculus I & II**
  Primary Texts: Calculus by James Stewart , *Calculus A Complete Course* by Robert A. Adams & Christopher Essex

  Topics: Limits, Derivatives, Integrals, Sequences, Multivariable Calculus, Stokes' and Green's Theorems

---

Technical Skills

- **Programming:** Python, Bash, LaTeX
- **Systems:** Linux (LPIC-1/2 level), systemd, shell scripting
- **Security:** RSA, Diffie-Hellman, cryptographic attacks, CTF challenges
- **Tools:** Git, Vim, Joplin, Pandoc

Selected Projects

Weiner's Attack on RSA

Implemented the continued fraction method to exploit RSA instances with small private keys. Explored rational approximations and convergents using Python.

Contact

- **Email:** ali.zare.mh@gmail.com
- **GitHub:** github.com/AL-IZ
- **LinkedIn:** linkedin.com/ali-zare-983463373
- **GPG Key:** Available on request