



Library Indian Institute of Science Education and Research Mohali



DSpace@IISERMohali / Thesis & Dissertation / Master of Science / MS-16

Please use this identifier to cite or link to this item: <http://hdl.handle.net/123456789/3830>

Title:	Primality testing and factorization
Authors:	Satender.
Keywords:	Primality Testing Factorization
Issue Date:	28-Jul-2021
Publisher:	IISERM
Abstract:	This thesis is a detailed study of primality testing and factorization algorithms. In the first part, we study about famous algorithms such as Fermat's factorization scheme, Robin-Miller Test, Solovay-Strassen Test, Continued Fraction Factoring Algorithm, Pollard-rho and $p-1$ test etc., then we study deterministic polynomial time AKS Algorithm. In, second part we study about Quadratic sieve algorithm and polynomial time lattice reduction algorithm, The LLL-Algorithm. Then we study in detail about polynomial factorization in finite field $\mathbb{Z}/p\mathbb{Z}$ and in field of rationals, \mathbb{Q} . In the last part, we study polynomial factorization using the LLL-Algorithm.
URI:	http://hdl.handle.net/123456789/3830
Appears in Collections:	MS-16

Files in This Item:

File	Description	Size	Format	
MS16069.pdf		925.87 kB	Adobe PDF	View/Open

Show full item record



Items in DSpace are protected by copyright, with all rights reserved, unless otherwise indicated.