

MATH-504

Integer optimisation

Eisenbrand Friedrich

Cursus	Sem.	Type
Ing.-math	MA2, MA4	Opt.
Mathématicien	MA2	Opt.

Language of teaching	English
Credits	5
Session	Summer
Semester	Spring
Exam	Oral
Workload	150h
Weeks	14
Hours	4 weekly
Courses	2 weekly
Exercises	2 weekly
Number of positions	

Summary

The course aims to introduce the basic concepts and results of integer optimization with special emphasis on algorithmic problems on lattices that have proved to be important in theoretical computer science and cryptography during the past 30 years.

Content

1. Lattices
2. Minkowski's Theorem
3. The LLL algorithm
4. Breaking Knapsack Cryptosystems
5. Transference bounds
6. Integer Programming in fixed dimension
7. Voronoi cells and single exponential time algorithms for shortest and closest vector
8. Polynomial-time factorization in $\mathbb{Q}[x]$

Learning Prerequisites**Recommended courses**

- Linear algebra 1+2
- Introduction to Algorithms or Discrete Optimization

Assessment methods

Oral Exam

Resources**Bibliography**

1. Thomas Rothvoss, Integer Optimization and Lattices
2. Oded Regev, Lattices in Computer Science, Lecture Notes