Math 228Y: Algorithms in Algebra and Number Theory

Fall 2021

Syllabus

Location: Science Center 310 (FAS)
Course website: `https://fabiangundlach.org/21-fall/228Y/`
Times: Tuesdays and Thursdays 12:00–1:15pm

Instructor
Fabian Gundlach
`gundlach@math.harvard.edu`
Office hours:
time: TBD
in Science Center 233

Prerequisites

This is a graduate topics course. Undergraduates are welcome.

We will use some algebra (finite fields, Galois groups) and algebraic number theory (for example from course 129; number fields, rings of integers, the class group, the unit group, decomposition of prime ideals, the p-adic numbers). Only a basic background in computer science will be needed. (Mostly, you need to be familiar with analyzing running times of algorithms.) You might find it interesting to implement the algorithms discussed in this course, but this is not required, and you're welcome to view the course as purely theoretical.

Tentative list of topics

In this course, we will explore some methods for designing efficient algorithms that solve basic questions in algebraic number theory (and perhaps algebraic geometry). Below, you can find a list of topics I am planning to discuss. (The list is tentative, especially regarding the topics in the bottom, some of which we will probably skip. The selection of topics also depends on your interests and background!)

- Basic algorithms in $\mathbb{F}_p[X]$ and $\mathbb{Z}$ (multiplication, division, greatest common divisor, ...)
- Factoring polynomials (over finite fields such as $\mathbb{F}_p$, local fields such as $\mathbb{Q}_p$, global fields such as $\mathbb{Q}$)
- Lattice algorithms (reduced lattice basis, in particular LLL reduction)
- Number field algorithms (determining the ring of integers, splitting behaviours of primes, the class group, the unit group, enumerating number fields, ...)
- Primality testing (through computational group theory)
- Factoring integers
- Counting prime numbers $p \leqslant n$ (recursively, or using analytic number theory)
- Computing Galois groups of field extensions
- Counting points on elliptic curves over $\mathbb{F}_p$ (Schoof's algorithm)
- Computational algebraic geometry (determining the dimension of a variety, number of irreducible components, ...)

References

There is no official textbook for this course. Some of the material can be found in the book "A course in computational algebraic number theory" by Henri Cohen. (The course will be more theoretical in nature than Cohen's book, so we won't cover implementation details.) Another good reference is "Computational Algebraic Number Theory" by Michael Pohst. For some of the things early in the semester, you can look at "Fast multiplication and its applications" by Daniel J. Bernstein.

I will try to give additional references for topics not covered in the book when we get to them in class.

Grading

Homework will probably[1] not be graded and the final grade will be entirely based on a final paper (10–15 pages) on a topic related to the class material.

Please acknowledge collaborators and other sources.

[1] assuming the course is not assigned a grader