# Computational Discrete Mathematics: Handout 00

Curtis Bright

September 9, 2021

## 1 Welcome to Computational Discrete Mathematics

This class will provide a broad introduction to computational discrete mathematics.

At its core this class will cover *how to effectively do mathematics on computers*. This involves topics like such as:

- Using a computer algebra system like Sage or Maple
- Algorithms for performing arithmetic on polynomials and arbitrarily large integers
- Solving linear Diophantine equations and the extended Euclidean algorithm
- Efficient modular arithmetic and the Chinese remainder algorithm
- Polynomial evaluation and interpolation and Karatsuba's multiplication algorithm
- Primality testing and factorization
- Fast multiplication and the discrete Fourier transform
- Fast division and Newton iteration
- Satisfiability solving and the Davis–Putnam–Logemann–Loveland procedure

A number of applications of these topics will be discussed, such as to coding theory, cryptography, and computer-assisted proofs.

**Instructor**: Curtis Bright
**Course Code:** COMP8920-2-R-2021F Selected Topics
**Class:** Thursdays 2:30–5:20 PM (online)
**Webpage:** Blackboard

### 1.1 Assessment

Assessment for the course will be based on a few things:

- Completing implementations of some of the algorithms that we discuss or related exercises (30%)
- Presenting topic(s) related to the course that are of interest to you (20%)
- A final project that will consist of reviewing a paper or collection of papers and writing an explanatory report of around 10 pages (50%)

### 1.2 References

There is no required textbook for the course, but the following books are good references:

- Modern Computer Algebra by Joachim von zur Gathen and Jürgen Gerhard

- A Computational Introduction to Number Theory and Algebra by Victor Shoup (freely available)
- Prime Numbers: A Computational Perspective by Richard Crandall and Carl Pomerance

The lecture notes will be posted on Blackboard.

### 1.3 Software

This class will mostly use the computer algebra system Sage which is freely available and runs on Linux, Windows, and MacOS. Some topics may be covered using Maple, a commercial computer algebra system developed by Maplesoft. You can choose whichever system you prefer to use. Maple has a free trial and I can provide you with a discount code if you are interested in purchasing an indefinite license or a license for the term.