Lattices
Algorithms, Complexity, and Cryptography Boot Camp

Lectures by Various
Scribed by Ben Burns

Simmons Institute – UC Berkeley

January 2020

Contents

1 Mathematics of Lattices – Daniele Micciancio (UCSD)

1.1 Point Lattices and Lattice Parameters (Point) lattices are useful in particular algorithm instances. For example, every prime $p \equiv 1 \pmod 4$ can be congruent to the sum of two squares can be formulated as the existence of a lattice point in a 2D lattice. Additionally breaking low-exponent RSA, coding theory, optimization, and building cryptographic functions.