Lattices, modularity, and crypto

Pi: Stephen D. Miller, Rutgers University
http://www.math.rutgers.edu/~sdmiller

Lattices arise in cryptography:

- In attacking cryptosystems (e.g., Knapsack, variants of RSA)
- Constructing new cryptosystems (e.g., for homomorphic encryption)

Fundamental problem: **shortest vector**

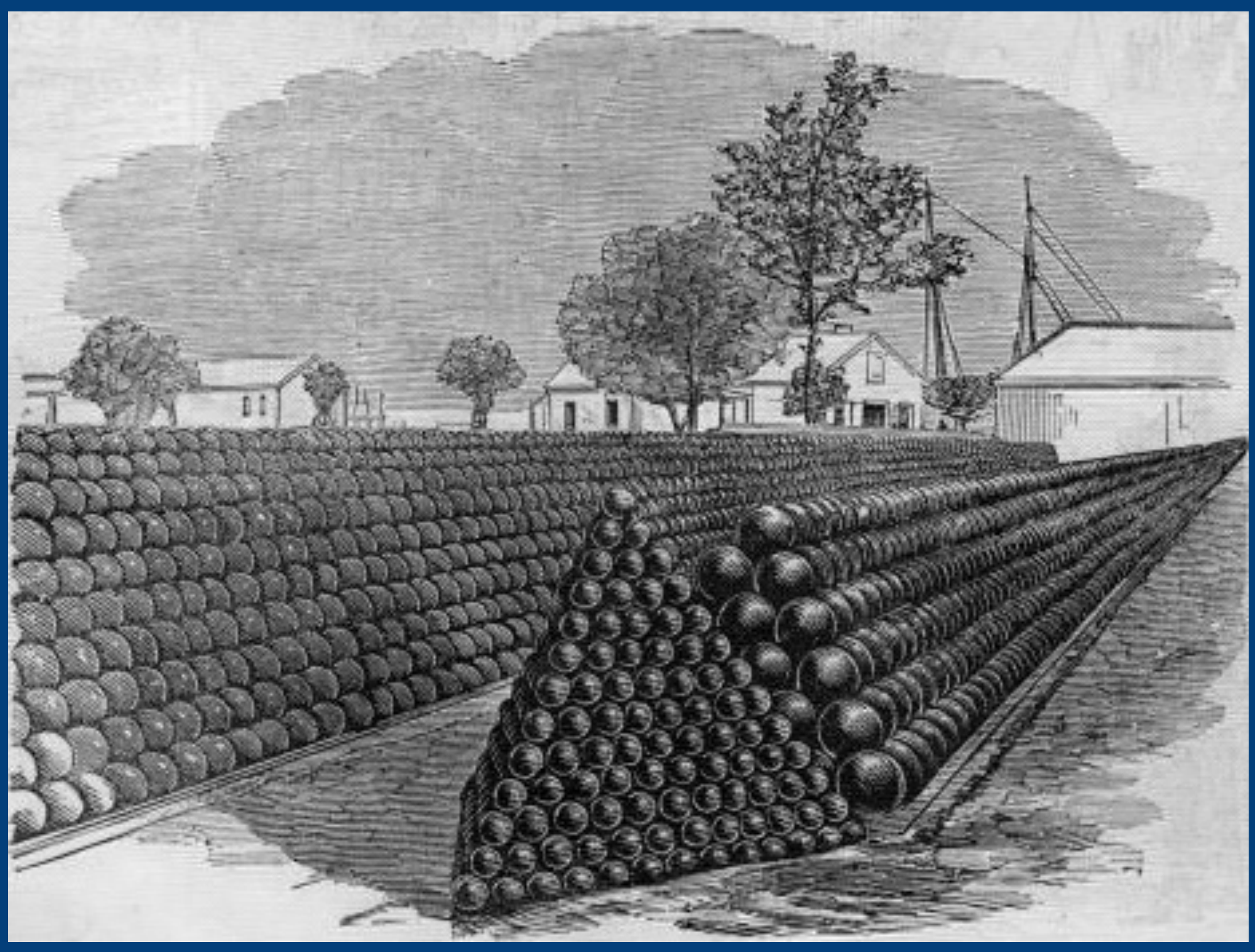
- Hard computational problem
- Related to classical *sphere packing problem* of how many balls fit into a large box.

Do we understand how short it can be?

Related question: energy minimization

Given a potential function and a fixed density of points, what configuration of points in $\mathbb{R}^d$ minimizes energy?

In d=3: why do crystals form in nature?



The densest packing in $\mathbb{R}^3$

Analytic Number Theory and Modular Forms are Applicable:

- Cohn-Elkies approach using Poisson sum (1999)
- Cohn-Miller: found rational numbers, e.g., Bernoulli number $\frac{691}{2730}$ in Taylor expansions (2016)
- Viazovska (2016): Modular form construction, solves sphere packing in $\mathbb{R}^8$
- Cohn-Kumar-Miller-Radchenko-Viazovska (2016): solves sphere packing in $\mathbb{R}^{24}$

Recent Progress: Solution in $\mathbb{R}^{24}$

The densest sphere packing in 24 dimensions has density exactly $\frac{\pi^{12}}{12!}$. It is provided by centering spheres of radius 1 at each vector of the Leech lattice.

Universal optimality of E_8

Cohn-Kumar-Miller-Radchenko-Viazovska (2016):

If $f\colon \mathbb{R}_{>0} \to \mathbb{R}_{>0}$ is "completely monotonic" ($(-1)^n f^{(n)}(x) \geq 0, \forall n \geq 0$) then the E_8 lattice minimizes potential energy for f among all point configurations density 1 in $\mathbb{R}^8$.

(Implies sphere packing.)

Uniqueness:

No other periodic sphere packing even equals the density of one provided by the Leech lattice.

(Removing a single sphere does not change density, so some aperiodic ones do.)

Other lattice results

Method to extend Boneh-Durfee's small-exponent RSA attacks to higher exponents.

Interested in meeting the PIs? Attach post-it note below!

National Science Foundation
WHERE DISCOVERIES BEGIN

The 3rd NSF Secure and Trustworthy Cyberspace Principal Investigator Meeting
January 9-11, 2017
Arlington, Virginia