Cryptography 4/6

Reagan Shirk

April 6, 2020

Project

- Sorry to any of my friends in the grad section that read my notes, but I'm in the undergrad section so I haven't been listening to anything about this project
- Good luck and godspeed

The Shortest Vector

- If we have an orthogonal base, then the shortest vector $\leq$ determinant$^{\frac{1}{n}}$
- On average, the shortest vector has length $\sqrt{\frac{n}{2e\pi}}\det(L)^{\frac{1}{n}}$. This is the Gauss Heuristic
- The Minkowski Convex Body Theorem sais that the shortest vector must have length less than $\sqrt{\frac{2n}{e\pi}}\det(L)^{\frac{1}{n}}$
- Something (I don't know what) works well when the Minkowski Convex Body Theorem is much less than the Guass Heuristic
- We can Google "sage LL" and we'll find a page that has a lot of useful information about running the LL algorithm in sage (useful for the project I think)

Lattice Reduction at Dimension 2 (Gauss Reduction)

- Basically a Euclidean Algorithm at Dimension 2
- I don't entirely understand what he's talking about, at least not well enough to describe it in text, but I guess I'll try
- You have four vectors, b_1 and b_2, b_1^* and b_2^*
  - We know that $b_1 = b_1^*$, but we want b_2^* to be orthogonal to b_2
  - Somehow we know that

$$\langle b_2^*, b_2 \rangle = 0$$

$$\langle b_2 - \mu b_1, b_1 \rangle = 0$$

$$\mu = \frac{\langle b_1, b_1 \rangle}{\langle b_1, b_1 \rangle}$$

    I don't think that that value for μ could possibly be correct but that's what it looked like so that's what I'll go with for now