Math 116 Spring 2022
Homework 8

Due Friday, May 20th

Sage instructions

- `v=vector([1,2])` sets `v` to be the (row) vector $(1,2)$, and `v[0]` returns the first entry of `v`, which is `1`.
- `M=Matrix([v1,v2])` sets `M` to be the matrix whose first row is the row vecor `v1` and second row is the row vector `v2`.
- `det(M)` is the determinant of a matrix `M`.
- `v.norm()` is the norm of a vector `v`
- `v1.dot_product(v2)` is the dot product of `v1` and `v2`
- `round(t)` is the nearest integer to the floating point number `t`. Unfortunately, `round` doesn't work on vectors. To round every entry of a vector, you can use:

  ```
  rounded_v = vector((round(e) for e in v)).
  ```
- `A.solve_left(y)` solves `xA = y`.

Problem 1. Read Section 7.7

Problem 2. (7.18 with Sage) Alice uses the GGH cryptosystem with private basis

$$\mathbf{v}_1 = (4, 13), \quad \mathbf{v}_2 = (-57, -45),$$

and public basis

$$\mathbf{w}_1 = (25453, 9091), \mathbf{w}_2 = (-16096, -5749).$$

(a) Compute the determinant of Alice's lattice and the Hadamard ratio of the private and public bases.

(b) Bob sends Alice the encrypted message e = (155340, 55483). Use Alice's private basis to decrypt the message and recover the plaintext. Also determine Bob's random perturbation r.

(c) Try to decrypt Bob's message using Babai's algorithm with the public basis $\{\mathbf{w}_1, \mathbf{w}_2\}$. Is the output equal to the plaintext?

Problem 3. Let $\mathbf{v}_1 = (1,1)$ and $\mathbf{v}_2 = (2, 0.5)$. Apply Gaussian lattice reduction by hand to compute the new basis $\mathbf{w}_1$, $\mathbf{w}_2$.

What is the Hadamard ratio of $\{\mathbf{v}_1, \mathbf{v}_2\}$? What is the Hadamard ratio of $\{\mathbf{w}_1, \mathbf{w}_2\}$? (Use a computer for this.)

Problem 4. (7.45(a), with Sage) Apply Gauss's lattice reduction algorithm (Proposition 7.66) to solve SVP for the two-dimensional lattice with basis

$$\mathbf{v}_1 = (120670, 110521) \quad \text{and} \quad \mathbf{v}_2 = (323572, 296358).$$

How many steps does the algorithm take? What is the Hadamard ratio of the input? What is the Hadamard ratio of the output?