Lecture 25 Lattice Cryptography §7.4

So historically:

- RSA first adopted
  - Discovered in 1973 at GCHQ
  - Publically described 1977
  - Patented Sept 20, 1983
  - Expired 2000
- Diffie-Hellman
  - Discoverd in 1969 at GCHQ
  - Published in 1976
  - Patented 1977
  - Expired Sept 6 1997
- Elliptic Curve Diffie-Hellman
  - Suggested in 1985
  - Widely adopted in 2004/2005.

Quantum computers with sufficiently many qubits can break all of these crypto systems.

Best existing quantum computers:

$\sim 50 - 100$ qubits

Needed to break good modern cryptography:

~ 1000 qubits.

→ Want quantum secure cryptography.

NIST use both ECDH & Lattice cryptography.

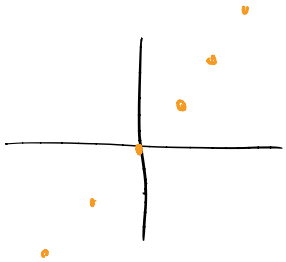
Lattices

Def A lattice in $\mathbb{R}^m$ is the set of integer linear combinations $a_1 v_1 + \cdots + a_n v_n$ where $a_i \in \mathbb{Z}$ & $\{v_1, \ldots, v_n\}$ is linearly independent over $\mathbb{R}$.

"$\dim L$" = "rank L" $= n$.

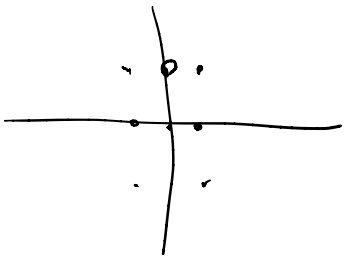
$\{v_1, \ldots, v_n\}$ is called a basis of L.

Ex. (1) $L_1 = \mathbb{Z}(1,1) \subset \mathbb{R}^2$ rank 1



(2) $L_2 = \mathbb{Z}(0,1) + \mathbb{Z}(\frac{1}{2},1)$

$= \mathbb{Z}(\frac{1}{2},0) + \mathbb{Z}(0,1)$



Prop Any two bases of a lattice differ by a matrix w/ integer entries and determinant ± 1.

Ex
$$\begin{pmatrix} 0 & 1/2 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1/2 & 0 \\ 0 & 1 \end{pmatrix} \underbrace{\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}}$$

integer entries

$\det = -1$.

Proof Let $\{v_1, \dots, v_n\}$ & $\{w_1, \dots, w_n\}$ be two bases of a lattice $L \subset \mathbb{R}^m$.

Since $w_i \in L$ it is possible to write

$$w_1 = a_{11} v_1 + a_{12} v_2 + \cdots + a_{1n} v_n$$

$$\vdots$$

$$w_n = a_{n1} v_1 + \cdots + a_{nn} v_n$$

where each $a_{ij} \in \mathbb{Z}$.

So $A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix}$

Satisfies $w_i = v_i A$.

Similarly there is a matrix B s.t. $v_i = w_i B$.

So $v_i AB = v_i$ & $w_i BA = w_i$

So $AB = BA = Id$.

$\Rightarrow \det(AB) = 1 = \det(A)\det(B)$.

$\Rightarrow \det(A) = \pm 1$.

□

$GL_n(\mathbb{Z})$ → the general linear group

$$= \left\{ \begin{array}{l} n \times n \text{ matrices with integer entries} \\ \& \det \in \underline{\mathbb{Z}^\times = \{1, -1\}} \end{array} \right\}.$$

units of $\mathbb{Z}$.

Ex $v_1 = \begin{pmatrix} 1 \\ 2 \\ 1 \end{pmatrix}$, $v_2 = \begin{pmatrix} 1 \\ -1 \\ 1 \end{pmatrix}$, $v_3 = \begin{pmatrix} 4 \\ 2 \\ 3 \end{pmatrix}$

$w_1 = \begin{pmatrix} 2 \\ 1 \\ 1 \end{pmatrix}$, $w_2 = \begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix}$, $w_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$

Question $\mathbb{Z}\{v_1, v_2, v_3\} \overset{?}{=} \mathbb{Z}\{w_1, w_2, w_3\}$

Answer Find change of basis matrix, then check if A has integer entries & $\det(A) = \pm 1$.

$$\begin{pmatrix} 1 & 1 & 4 \\ 2 & -1 & 2 \\ 1 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 2 & -1 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} A$$

$$\Rightarrow A = \underbrace{\begin{pmatrix} 2 & -1 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}^{-1}}_{M} \begin{pmatrix} 1 & 1 & 4 \\ 2 & -1 & 2 \\ 1 & 1 & 3 \end{pmatrix}$$

$$M^{-1} = \frac{1}{3}\begin{pmatrix} 1 & 1 & 0 \\ -1 & 2 & 0 \\ -1 & -1 & 3 \end{pmatrix}$$

$$A = \frac{1}{3}\begin{pmatrix} 1 & 1 & 0 \\ -1 & 2 & 0 \\ -1 & -1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 1 & 4 \\ 2 & -1 & 2 \\ 1 & 1 & 3 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 0 & 2 \\ 1 & -1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$

- A has integer entries
- $\det(A) = -1 + 2 = 1$

$\rightsquigarrow A \in GL_n(\mathbb{Z})$. $\Rightarrow \mathbb{Z}\{v_1, v_2, v_3\} = \mathbb{Z}\{w_1, w_2, w_3\}$.

Lecture 26 Lattices §7.4

Recall

Def A lattice is a discrete subgroup of $(\mathbb{R}^n, +)$.

In other words:

Def A lattice is the set of $\mathbb{Z}$-linear combinations $a_1 v_1 + \cdots + a_n v_n$ of some basis $\{v_1, \ldots, v_n\}$.

Prop Two bases of a lattice differ by an elt of $GL_n(\mathbb{Z})$.

Ex $v_1 = \begin{pmatrix} 1 \\ 2 \\ 1 \end{pmatrix}$, $v_2 = \begin{pmatrix} 1 \\ -1 \\ 1 \end{pmatrix}$, $v_3 = \begin{pmatrix} 4 \\ 2 \\ 3 \end{pmatrix}$

$w_1 = \begin{pmatrix} 2 \\ 1 \\ 1 \end{pmatrix}$, $w_2 = \begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix}$, $w_3 = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$.