$$N = \frac{853}{2^{10}} = \frac{853}{1024} = 0 + \cfrac{1}{1 + \frac{171}{853}}$$

$$= 0 + \cfrac{1}{1 + \cfrac{1}{4 + \frac{169}{171}}}$$

$$= 0 + \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{1}{1 + \frac{2}{169}}}}$$

Lattice. **Def^n.** A lattice in $\mathbb{R}^n$ (or $\mathbb{F}_p^n$)

is any set of the form

$$\Lambda = \left\{ \sum a_i \vec{x}_i \; : \; a_i \in \mathbb{Z} \right\}$$
$$= \vec{x}_1 \mathbb{Z} + \cdots + \vec{x}_n \mathbb{Z}$$

for a fixed basis $\vec{x}_1, \ldots, \vec{x}_n$ of $\mathbb{R}^n$

$\Rightarrow$ any $v \in \Lambda$ has a unique way to express it in terms of basis

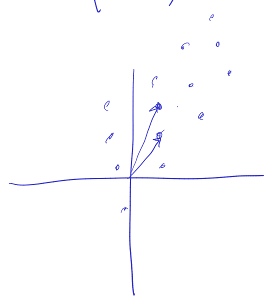
---

Represent a lattice: $\Lambda = \vec{x}_1 \mathbb{Z} + \cdots \vec{x}_n \mathbb{Z}$

then we write a matrix w/ colums $\vec{x}_1, \ldots, \vec{x}_n$

$$M = \begin{pmatrix} \uparrow & \uparrow & & \uparrow \\ x_1 & x_2 & \cdots & x_n \\ \downarrow & \downarrow & & \downarrow \end{pmatrix} \qquad n \times n \text{ matrix}$$

eg. $\begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix}$



Change Basis: (Preserves Λ)

You can:
- reorder the basis elements
- add a multiple of one basis elt to another
- in general, any matrix w/ $\mathbb{Z}$ entries & $\det = \pm 1$ will give a valid change of basis

Ex.
$$\Lambda = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \mathbb{Z} + \begin{pmatrix} 0 \\ 1 \end{pmatrix} \mathbb{Z} \qquad M_\Lambda \cdot N = M'_\Lambda$$
$$= \begin{pmatrix} 1 \\ 2 \end{pmatrix} \mathbb{Z} + \begin{pmatrix} 0 \\ 1 \end{pmatrix} \mathbb{Z}$$
$$= \begin{pmatrix} 1 \\ 2 \end{pmatrix} \mathbb{Z} + \begin{pmatrix} 1 \\ 3 \end{pmatrix} \mathbb{Z}$$

$$\underset{M_\Lambda}{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}} \cdot \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \underset{M'_\Lambda}{\begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix}}$$

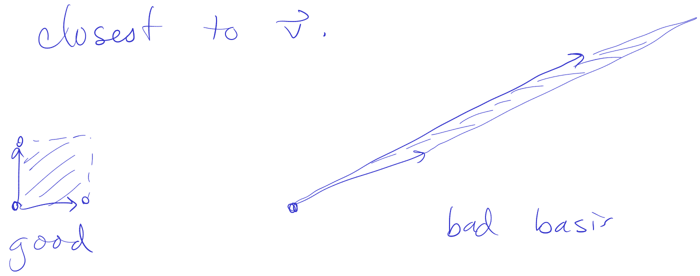
$$\begin{pmatrix} | & | \\ v_1 & v_2 \\ | & | \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} | & | \\ v_2 & v_1 \\ | & | \end{pmatrix}$$

$$\begin{pmatrix} | & | \\ v_1 & v_2 \\ | & | \end{pmatrix} \cdot \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \underbrace{\begin{matrix} | \\ v_1 \\ | \end{matrix}} & \underbrace{k \begin{pmatrix} | \\ v_1 \\ | \end{pmatrix} + 1 \begin{pmatrix} | \\ v_2 \\ | \end{pmatrix}} \end{pmatrix}$$

Hard Lattice Problems:

① <u>Shortest Vector Problem</u>: Given a lattice (in a potentially bad basis), find the shortest non-zero vector in the lattice (as a linear combination of the basis).

② <u>Closest Vector Problem</u>: Given a lattice (in a pot. bad basis), and given $v \in \mathbb{R}^n$, find the vector in the lattice closest to $\vec{v}$.

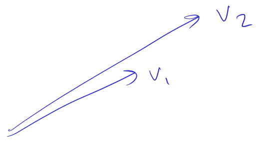


Cryptographic dims:
$n \approx 300 - 1500$.

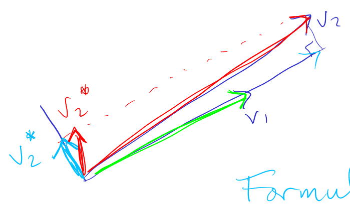
Lattice Reduction in 2 D.

<u>goal</u>: find a short vector in $\mathcal{L}$.
(find a good basis).

Suppose $\|v_1\| \leq \|V_2\|$



Idea: make them more perpendicular



Gram-Schmidt Formula

closest integer

$$V_2^* = \vec{V}_2 - \left[\frac{\vec{V}_1 \circ \vec{V}_2}{\|V_1 \circ V_1\|}\right] \vec{V}_1$$

New basis: $\vec{V}_1, \vec{V}_2^*$ (improved)

Swap so $\|V_2^*\| < \|V_1\|$

& repeat

<u>Example</u>. $v_1 = \binom{17}{5}$, $v_2 = \binom{19}{10}$

$\|v_1\|^2 = 17^2 + 5^2 = 314 \qquad \|v_2\|^2 = 19^2 + 10^2 = 461$

① $\|v_1\| \leq \|V_2\|$ ✓

$$V_2^* = V_2 - \left[\frac{V_2 \circ V_1}{V_1 \circ V_1}\right] V_1 = \binom{19}{10} - \left[\frac{19 \cdot 17 + 10 \cdot 5}{314}\right] \binom{17}{5}$$

$$= \binom{19}{10} - \left[\frac{373}{314}\right] \binom{17}{5}$$

$$= \binom{19}{10} - 1 \cdot \binom{17}{5} = \binom{2}{5}$$

New basis $\binom{17}{5}, \binom{2}{5}$

② $v_1 = \binom{2}{5} \leq v_2 = \binom{17}{5}$ (swapped so shortest 1st)

$$v_2^* = v_2 - \left[\frac{17\cdot 2 + 5\cdot 5}{29}\right]\binom{2}{5} = \binom{17}{5} - 2\cdot\binom{2}{5} = \binom{13}{-5}$$

③ $v_1 = \binom{2}{5} \leq v_2 = \binom{13}{-5}$

$$v_2^* = v_2 - \left[\frac{1}{29}\right] v_1 = v_2$$

NO IMPROVEMENT!

DONE.

Thm. This will always terminate, & the resulting basis will include the shortest non-zero vector.